PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 04 September 2001 (04.09.01)	
International application No. PCT/US00/27782	**Applicant's or agent's file reference** 249/118-PCT
International filing date (day/month/year) 06 October 2000 (06.10.00)	**Priority date** (day/month/year) 07 October 1999 (07.10.99)
Applicant O'GORMAN, Lawrence et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

07 May 2001 (07.05.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Maria KIRCHNER

Telephone No.: (41-22) 338.83.38

10/089987

CORP
POSTAGE

RECEIVED
APR 08 2002
USPTO MAIL CENTER

OIPE JC15
APR 05 2002
PATENT & TRADEMARK OFFICE

PCT

* E L 3 5 6 0 7 9 6 3 1 U S *

EXPRESS MAIL UNITED STATES POSTAL SERVICE™ OFFICES LYON & LYON LLP A LIMITED LIABILITY PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS

POST OFFICE TO ADDRESSEE

ORIGIN (POSTAL USE ONLY)

PO ZIP Code: 92037	Day of Delivery: ☐ Next ☐ Second	Flat Rate Envelope ☐	4225 Exe... La J...
Date In: Mo. 04 Day 05 Year 02	☐ 12 Noon ☐ 3 PM	Postage: $ 7.45	
Time In: ☐ AM 01 ☐ PM	Military: ☐ 2nd Day ☐ 3rd Day	Return Receipt Fee: COMMISSIONER FOR PATENTS	
Weight: 1 lbs. 12 ozs.	Int'l Alpha Country Code	COD Fee	Insurance Fee: WASHINGTON D.C. 20231
No Delivery: ☐ Weekend ☐ Holiday	Acceptance Clerk Initials: MA	Total Postage & Fees: $ 20.45	

DELIVERY (POSTAL USE ONLY)

Delivery Attempt: Mo. Day	Time: ☐ AM ☐ PM	Employee Signature
Delivery Attempt: Mo. Day	Time: ☐ AM ☐ PM	Employee Signature
Delivery Date: Mo. Day	Time: ☐ AM ☐ PM	Employee Signature
Signature of Addressee or Agent: X		
Name - Please Print: X		

USPTO MAIL CENTER
APR 05 2002
DATE IN

Addressee Copy
EP11-F July 1997

CUSTOMER USE ONLY

TO FILE A CLAIM FOR DAMAGE OR LOSS OF CONTENTS, YOU MUST PRESENT THE ARTICLE, CONTAINER, AND PACKAGING TO THE USPS FOR INSPECTION.

☐ **WAIVER OF SIGNATURE** (Domestic Only): Additional merchandise insurance is void. Waiver of signature is required. I wish delivery to be made without obtaining signature of addressee or addressee's agent (if delivery employee judges that article can be left in secure location) and I authorize that delivery employee's signature constitutes valid proof of delivery.

NO DELIVERY ☐ Weekend ☐ Holiday

Customer Signature

FROM: (PLEASE PRINT) PHONE ( )

LYON & LYON LLP
4225 EXECUTIVE SQ STE 800
LA JOLLA CA 92037-9150

TO: (PLEASE PRINT) PHONE ( )

ASSISTANT COMMISSIONER FOR
PATENTS
WASHINGTON DC 20231-0002

PATENT
BOX UTILITY APPLICATION

VERIDICOM 249/118 US-SWW

FOR PICKUP OR TRACKING CALL 1-800-222-1811 www.usps.gov EMS

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/24700 A1

(51) International Patent Classification[7]: A61B 5/117, G07C 9/00, G06K 9/00

(21) International Application Number: PCT/US00/27782

(22) International Filing Date: 6 October 2000 (06.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/158,423 7 October 1999 (07.10.1999) US

(71) Applicant *(for all designated States except US)*: VERIDICOM, INC. [US/US]; 2040 Martin Avenue, Santa Clara, CA 95050-2702 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: O'GORMAN, Lawrence [US/US]; 18 Albright Circle, Madison, NJ 07940 (US). SCHUCKERS, Stephanie [US/US]; 1282 Forman Drive, Morgantown, WV 26508 (US). DERAKHSHANI, Reza [IR/US]; Apt. #K-311, 1056 Van Voorhis Road, Morgantown, WV 26505 (US). HORNAK, Lawrence [US/US]; 133 Poplar Drive, BRM, Morgantown, WV 26505 (US). XIA, Xiongwu [CN/US]; 31 Scotto Place, South Brunswick, NJ 08810 (US). D'AMOUR, Michael [US/US]; 2040 Martin Avenue, Santa Clara, CA 95050 (US).

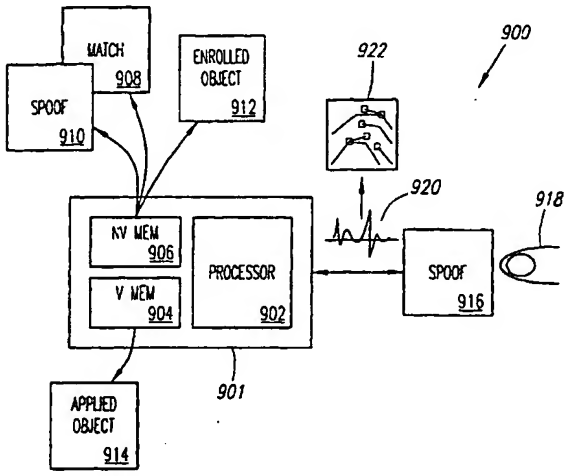
(74) Agents: HEMMINGER, Steven, D. et al.; Lyon & Lyon LLP, Suite 4700, 633 West Fifth Street, Los Angeles, CA 90071-2066 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: SPOOF DETECTION FOR BIOMETRIC SENSING SYSTEMS



(57) Abstract: A biometric sensing system and techniques are disclosed for detecting spoofs of a living finger. In accordance with an embodiment of the invention, unique biological and physical characteristics of a finger are captured by a fingerprint sensor over a sequence of images and interpreted from the captured images. The characteristics are extracted from an electrical representation of the finger in what, in the past, was considered "noise" in the electrical representation. According to one embodiment, the system comprises an image capture device configured to sample an applied object and create an electrical representation of the applied object and a spoof detection module configured to analyze the electrical representation of the applied object for relative intensity, density, geometric, or temporal anomalies indicative of a non-living applied object. Methods are disclosed for the same end, the methods including: average intensity, pixel density, rate of warming, ridge uniformity, ridge signal strength, water droplet differential, fingerprint vitality, and inverted spoof techniques.

WO 01/24700 A1

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *With international search report.*

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Process this Application in accordance with the

PATENT COOPERATION TREATY

TITLE OF THE INVENTION

Spoof Detection for Biometric Sensing Systems

APPLICANT

Veridicom, Inc.

2040 Martin Ave.

Santa Clara, CA 95050

U.S.A.

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to U.S. Provisional Application Serial No. 60/158,423, filed October 7, 1999, entitled, "Method and Apparatus for Determining a Living Fingerprint on a Fingerprint Sensor," which is incorporated herein by reference in its entirety, and to which priority is claimed.

BACKGROUND

1. Field of the Invention.

The invention relates to biometric sensors, and more particularly to fingerprint sensors and techniques for distinguishing between living and non-living fingers placed on a sensor.

2. Background Information.

Fingerprint identification and authentication systems rely on a user's unique fingerprint to identify whether the user is authorized to access the system. A significant challenge for fingerprint authentication systems is to prevent unauthorized access gained through the use of a spoof, i.e. a fingerprint from a non-living finger. A spoof can include an artificially produced fingerprint (e.g., a molded plastic or rubber 3-dimensional impression of a true fingerprint), a fingerprint from a finger of a dead person, or a fingerprint from a finger severed off of a live person. Each of these spoofs circumvents the fingerprint authentication process, as the spoof can be used separate from its legitimate owner.

One solution to this problem is to require the use of an accompanying password or personal identification number (PIN). All bank cards and most other tokens require both the

card and a PIN. This combination is a good defense against the spoof attack. Multi-factor authentication is required in many applications not only as a defense against spoofing, but also as an increased level of security.

However, multi-factor authentication has drawbacks. For example, the accounting or card issuing organization faces significant administrative cost in handling the secret codes and the card holders have to memorize the secret codes. In addition to the cost of managing the secret codes, the card issuing organization faces significant cost in handling the cards such as issuing new cards or dealing with lost cards and the card holders have to carry the cards which may be inconvenient to the users in certain situations. Therefore, it is advantageous to capitalize on the inherent benefit of identification through the user's fingerprint, which does not require the user to remember any passwords or to retain any tokens. Accordingly, there is a need to be able to distinguish between living fingers and spoofs, so as to ensure that only authorized persons will be able to access the protected system.

For example, one fairly simple way of illegally accessing an optical fingerprint system is with a photographic copy of a true fingerprint. Older optical fingerprint systems are unable to discriminate between a real fingerprint and a photocopy. To overcome this problem, some optical systems now use frustrated total internal refraction (FTIR), while others employ ultrasound technology. FTIR systems are designed to reflect light from surfaces of the skin directly in contact with the scanner (e.g. fingerprint ridges) and not to reflect light from those surfaces out of contact with the scanner (e.g. fingerprint valleys). Ultrasonic systems such as ones described in U.S. Patent No. 5,587,533 entitled "Surface Feature of Mapping Using High Resolution C-Scan Ultrasonography" of Schneider et al. issued December 24, 1996, direct ultrasonic waves to the object placed on the scanner and monitor the waves that are returned. Both types of optical systems can discriminate between a flat photocopy of a fingerprint and a true fingerprint having 3-dimensional depth. One shortcoming, however, with both of these optical systems is that they cannot distinguish between a living finger and a 3-dimensional finger molded from plastic or rubber, nor a dead from a living finger.

Other approaches are used for non-optical fingerprint authentication systems. For example, some fingerprint capture devices measure the subject's skin resistance and temperature. These measurements can then be compared to normal values for a living finger. If the measurements deviate from normal values, then the fingerprint is identified as a spoof.

The skin resistance and temperature safeguards, however, can easily be circumvented by warming up an artificial or dead finger or by designing an artificial finger with a resistance similar to a true finger.

Still other fingerprint authentication systems utilize other medical measurements to determine whether the fingerprint presented is from a living finger or a spoof. One such system is described in U.S. Patent No. 5,719,950, entitled "Biometric, Personal Authentication System" of Osten et al., issued February 17, 1998, which incorporates biological measurements, such as electrocardiograph signals and blood pressure, in conjunction with a fingerprint scan to determine whether the fingerprint presented originates from a living finger. Disadvantages of these systems include their complexity, large size and high cost. In addition, systems which probe medical signals of a person are highly intrusive.

There is a need, therefore, for an improved method for distinguishing a living finger from a spoof. In particular, the method should accurately discern between the two without being overly intrusive. The method also should not significantly increase the size or cost of the system.

SUMMARY OF THE INVENTION

A method and apparatus for employing spoof detection for a biometric sensing device is provided. The invention employs a number of computer implemented techniques designed to distinguish between a living and a non-living biometric, particularly a fingerprint. Anomalies of an electrical representation of a fingerprint, captured from the biometric sensing device, are analyzed using any number of steps designed to detect certain characteristics that are difficult to spoof and largely unique to a living finger.

According to one embodiment, a solid state fingerprint sensor is employed. One such solid state sensor is a capacitive sensor that captures fingerprints by electrical means. Depth is determined by electric field strength, which is inversely proportional to distance. Because capacitive fingerprint sensors require a three-dimensional object, they do not accept a photographic copy of a true fingerprint. In addition, in order for these sensors to capture a fingerprint, the finger or object presented to the sensor must have electrostatic characteristics similar to the skin on a living finger. This will eliminate fingerprints from plastic or rubber molded fingers, as these materials are non-conductive.

The method further relies on additional characteristics of living fingers that cannot be easily replicated by an artificial, dead or severed finger. For example, living skin has the

functions of excretion of substances through sweat glands and absorption of lipid-soluble substances. Sweat glands include pores which are small openings of the sweat ducts in the skin surface. Pore patterns are unique and they do not disappear, move, or spontaneously change over time. The sweat glands also produce unique characteristics of a living finger. For example, a living finger being a heat source, which warms up the sensor after it is placed on a fingerprint sensor; a living finger perspires; and the skin of a living finger is hydrophilic. Accordingly, the invention analyzes the electrical representation of the fingerprint for characteristics such as intensity or density, as well as, in some embodiments, spatial, geometric, and/or temporal anomalies largely inconsistent with a living finger.

The above characteristics may be observed over a series of captured images. With an increase in temperature, a living finger perspires. Therefore, areas surrounding pores in the finger produce stronger signals. Because the skin of a living finger is hydrophilic, it absorbs liquid. Thus, even with perspiration, a living finger placed on the sensor is capable of generating an image that exhibits good differentiation between the ridges and valleys of the finger.

According to one embodiment, the invention is a biometric sensing system including an image capture device configured to sample an applied object and create an electrical representation of the applied object and a spoof detection module configured to analyze the electrical representation of the applied object for relative intensity, density, geometric, or temporal anomalies indicative of a non-living applied object. Various methods for the spoof detection module are described below.

In one embodiment, the method includes capturing a sequence of images of the applied object from the sensor and calculating an average intensity for each image. In one embodiment, the average intensity is calculated based on the entire image. In another embodiment, the average intensity is calculated based on a portion of the image. In still another embodiment, the average intensity is ON-pixel normalized, meaning that only pixels having a signal exceeding a predetermined threshold value that indicates a fingerprint ridge are used for this calculation. The method further includes successively comparing the average intensities of the sequence of images to determine whether they vary beyond a predetermined threshold amount. If the averages vary beyond the threshold amount, then the system accepts the image as coming from a live person. If the averages do not vary beyond the threshold amount, then the system acquires an additional image of the applied object and calculates the average intensity for that image.

The average intensity of the additional image is compared with the prior averages for the sequence of images to determine whether the averages vary beyond the threshold amount. If the averages still do not vary beyond the threshold amount, then the system repeats the steps of acquiring another image, calculating the average intensity for that image, and comparing that average with the previous ones, until the maximum number of images have been captured. At that point, the system rejects the applied object as being a spoof, rather than a living finger.

In another embodiment, the density of the ON-pixels is calculated over a sequence of images instead of average intensity. In one embodiment, maximum and minimum pixel values for an image (either the entire image or a selected portion of an image) are determined. A mid-value is then determined. A pixel with a value greater than the mid-value is considered to be an ON-pixel. The number of ON-pixels over the number of total pixels (in either the entire image or a selected portion of an image) is the density of an image. The density of each image in the sequence is successively compared with the density of the previous image. An increase in density over the sequence of images exceeding a predetermined threshold amount indicates that the object is from a live person. Otherwise, the object is a spoof.

In still another embodiment, the average intensity is calculated separately for the middle fingerprint portion and the outer fingerprint portion for each image in the sequence of images. Each average intensity of the middle fingerprint portion is successively compared with the average intensity of the middle fingerprint portion of a previously captured image. Likewise, each average intensity of the outer fingerprint portion is successively compared with the average intensity of the outer fingerprint portion of a previously captured image. If the average intensity for the outer fingerprint portion increases faster than the average intensity for the middle fingerprint portion, then the fingerprint is determined to be coming from a spoof. Calculating and comparing the rate of increase for the middle fingerprint portion and the outer fingerprint portion protects the system from falsely accepting an artificially warmed spoof. This is because the middle fingerprint portion warms up faster than the outer fingerprint portion for a living finger while the outer fingerprint portion warms up faster than the middle fingerprint portion for an artificially warmed spoof.

In an alternative embodiment, the density of the middle fingerprint portion and the density for the outer fingerprint portion are calculated and successively compared. If the

density for the middle fingerprint portion increases at a rate that is faster than the outer fingerprint portion, then the image is coming from a living finger.

In one embodiment, the rate of warming for the sequence of captured images is calculated and compared with the rate of warming of the finger during enrollment or during a previous successful verification. The rate of warming, in one embodiment, is calculated using average intensity. In an alternative embodiment, the rate of warming is calculated using density. Comparing the rate of warming for an applied object and a previously determined rate of warming prevents false acceptance of an artificially warmed spoof because the rate of warming of a living finger differs from the rate of warming of a spoof.

In one embodiment, the changes in intensity along the ridges are measured over a sequence of images. If the intensity along ridges increases in a spatially non-uniform way, then the image is accepted as coming from a live person because a spatially non-uniform increase in intensity along the ridges indicates pores emanating sweat which is an indicator of a living finger.

In an alternative embodiment, the nonuniformly increasing intensity is measured along the contours of ridges to obtain a linear sequence of intensity values. The linear sequence depends on the intensity along the ridge. For example, the typical ridge comprises pixels having intensities that increase as they get closer to a pore and decrease as they get further from the pore. Thus, the signal of the contour is typically sinusoidal and has a particular frequency. Since a spoof has no pores, the signal of the contour does not have a frequency related to pore-to-pore frequency. In other words, the signal from a spoof is not sinusoidal. In one embodiment, the intensity periodicity and nonuniformity of the pore-to-pore frequency content in a specific window are measured by Fourier transform.

In one embodiment, the signals for the ridges of the sequence of images are compared. If there are no changes in the signals along a ridge, then the system determines whether the signals are at a maximum. In addition to no signal change along a ridge, a maximum signal strength can indicate that a living finger that is wetted, a living finger that is saturated due to perspiration, or a spoof saturated with moisture. In one circumstance, the system accepts the image as coming from a living finger. In another embodiment, the system notifies the user to wipe excess moisture off the applied object or the sensor and to try again.

In one embodiment, water droplets are located and their sizes measured for each image in the sequence of images. In one embodiment, a water droplet image is a group of pixels having a width exceeding the width of a ridge (note that the ridge is narrow and long

while the water droplet is fat and short). The sizes of the water droplets are successively compared. The same or decreasing sizes can indicate that the object is a wetted spoof, or the object is a living finger with over-accumulation of surface moisture. The system rejects the fingerprint. Again, the system can instruct the user to wipe off excessive moisture from the applied object or sensor and try again.

In one embodiment, matching minutiae are further compared with respect to their minutia type, that is, endpoint or bifurcation. The ratio of mismatches of minutia type to the overall minutia matches is compared against a threshold amount. If the ratio exceeds the threshold value, then the sensed fingerprint is rejected as a spoof.

In still another embodiment, the same finger is to be disposed over on the sensor multiple times -- e.g. twice. A sequence of images are captured each time. The sequences of images are then compared. For a true finger, the first image in the second sequence exhibits characteristics closer to the last image in the first sequence while for a spoof, the first image in the second sequence exhibits characteristics closer to the first image in the first sequence.

In another embodiment, two-dimensional captured images are mapped into one-dimensional signals. Static (e.g. from one fingerprint image) and dynamic (e.g. temporal change of perspiration pattern of the skin) measures are then extracted and used for classification. The static and dynamic measures can include those detectable within the same signal derived from one fingerprint image and those observed in temporal transition from one signal to the next such as temporal changes over multiple image signals, respectively. The static measure can be used to detect variations in gray level due to darkening around the pores and the dynamic measure can be used to detect the changes caused by perspiration over time. These measurements are quantified to produce a sweating pattern.

In one embodiment, the calculated parameters, for example, the energy inside normal pore frequency window, total swing ratio, minimum/maximum growth ratio, last-first fingerprint signal difference mean and percentage change of standard deviations, are fed into a neural network. According to one instance, if the output of the neural network is in a predetermined range, then the applied object passes as coming from a living finger. In another instance, the predetermined range is positive. If the output of the neural network is in a second predetermined range, then it is determined whether a predetermined number of trials have been met. In one embodiment, the second predetermined range is negative. If the number of trials is less than a predetermined number of maximum trials, then the system prompts the user to wipe the applied object. The system then captures another sequence of

images. The system repeats the process until the predetermined number of maximum trials has been met, at which time the system rejects the fingerprint as coming from a spoof.

The methods are typically embodied in computer software product executed and/or interpreted by one or more processors. The processor(s) can be part of a network system, a stand-alone computer, an automated teller machine, a wireless telephone, or a smart card, for instance.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1, which comprises FIG. 1A and FIG. 1B arranged in a manner shown in the key to FIG. 1, is a flowchart of a method for distinguishing between a living finger and a spoof by calculating average intensities of a sequence of images.

FIG. 2 shows a block diagram of a fingerprint system.

FIG. 3, which comprises FIG. 3A and FIG. 3B arranged in a manner shown in the key to FIG. 3, is a flowchart of a method for distinguishing between a living finger and a spoof by calculating density of a sequence of images.

FIG. 4 is a flowchart of a method for distinguishing between a living finger and a spoof by calculating the average intensity change along a ridge.

FIG. 5 is a flowchart of a method for distinguishing between a living finger and a spoof by determining whether the average intensity changes along the ridges and whether the average intensities at the ridges are at a maximum value.

FIG. 6 is a flowchart of a method for distinguishing between a living finger and a spoof by comparing the size of water droplets on a sequence of images.

FIG. 7, which comprises FIG. 7A and FIG. 7B arranged in a manner shown in the key to FIG. 7, is a flowchart of a method for distinguishing between a living finger and a spoof based on perspiration characteristics.

FIG. 8 is a flowchart depicting a method for distinguishing between a living finger and an inverted spoof of the living finger.

FIG. 9A is a block diagram of an exemplary biometric sensing system.

FIG. 9B is a block diagram of a capacitive fingerprint sensor.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In accordance with the invention, computer implemented methods and associated apparatuses for distinguishing a living finger from a spoof are provided. A living finger, as

opposed to a fake or a dead finger, exhibits vitality, meaning that it has blood flow, perspiration, neuroactivity and other biological functions. For example, living skin has the functions of excretion of substances through sweat glands and absorption of lipid-soluble substances. Each square inch of skin includes approximately 600 sweat glands. Sweat glands include pores, which are small openings of the sweat ducts in the skin surface. Pore patterns are unique and they do not disappear, move, or spontaneously change over time. Typically, pore-to-pore distance is approximately 0.5 mm, or there are approximately 20.8 pores per centimeter (cm) on the ridge. The sweat glands produce some unique biological effects such as the production of heat and moisture (perspiration), as well as the absorption of moisture.

A living finger is a heat source. Therefore, after a living finger is placed on a fingerprint sensor, the finger will warm the sensor. This increase in sensor temperature over a sequence of images can indicate a living finger. In one embodiment, the temperature change is measured directly such as with a heat sensor or the equivalent. In another embodiment, the temperature change is measured indirectly. For instance, increasing temperature causes increasing surface moisture on the finger (due to perspiration).

A living finger perspires. Because moisture is conductive, conductivity increases with increasing moisture. Therefore, if measured by a resistive sensor, then resistance decreases can be observed and, if measured by a capacitive sensor, then capacitance increases can be observed. In addition to an increase/decrease in signal strength, the area of the increased/decreased signal strength expands as perspiration emanates from pore locations along the ridges.

Skin on a living finger is hydrophilic, that is, it absorbs water and other liquids applied at the surface of the skin. Hence, moistures are evenly distributed over the finger and when a living finger is wetted, either with liquid or from perspiration, a quality image having good differentiation between ridges and valleys of the finger may still be generated. This is opposed to a wetted spoof, which can be hydrophobic and tends to pool the moisture in the valleys, thereby yielding little or no ridge to valley differentiation.

Moreover, the texture of the skin has particular characteristics where transitions between ridges and valleys, i.e., at endpoints and bifurcations, occur.

In accordance with an embodiment of the invention, these unique biological and physical characteristics are captured by a fingerprint sensor over a sequence of images and interpreted from the captured images. They are not necessarily measured directly by

biosensors, but rather extracted from the electrical representation of the finger in what may have, in the past, been considered "noise" in the electrical representation.

SYSTEM OVERVIEW

FIGS. 9A-B are block diagrams of an embodiment of the biometric sensing system. Biometric sensing system 900 comprises a processing unit 901 and a sensor 916. The two are communicatively coupled, for instance, by a serial port, or a common bus. The processing unit 901 comprises a processor 902, such as a Motorola 6800 or 68000 series microprocessor. Further included in the processing unit is volatile memory 904 (e.g. RAM), in which temporary variables and executed program code can reside, and a non-volatile memory 906 (e.g., ROM, EPROM, EEPROM, or FLASH), in which persistent program code (to be later executed, for instance) and data reside.

According to one embodiment, the non-volatile memory 906 holds a minutia matching module 908, which is computer program code for finding matches between minutia of the electrical representation of an applied object 914 (a finger 918). An exemplary matching module is described in U.S. Patent Application Serial No. 09/354,929, filed November 17, 1999, entitled "Method and System for Fingerprint Template Matching," which is incorporated herein by reference in its entirety. Another matching module can include the techniques embodiment in U.S. Patent Application Serial No. 09/501,355, filed February 9, 2000, entitled "Biometric False Accept Detection," which is also incorporated herein by reference in its entirety.

An enrolled object 912, which was previously captured and verified, is also stored in non-volatile memory 906. One embodiment of a data structure that can be used to hold information representative of the enrolled object is described in PCT International Application Serial No. PCT/US00/18714, filed July 7, 2000, entitled "Multi-Dimensional Fingerprint Minutia Data Constellation," which is incorporated herein by reference in its entirety.

Furthermore, the non-volatile memory 906 includes and spoof detection module, which can also be computer program code, implementing the methods described in detail below, which distinguishes between a living applied object and a non-living applied object. (It is appreciated that the particular memory or component arrangement can vary -- for instance, the various modules and memories might not all be physically resident in a single

location, but can be distributed and "logically" arranged as depicted in FIG. 9A. The figure and description is intended to capture this logically arrangement.)

While the program code is ultimately embodied in a system as depicted, for instance, in FIG. 9A, the program code can be sequences of instructions for causing a processor (or distributed processors) to perform the functionalities described above (and more particularly below). The program code, or "software product", can be stored in a tangible medium, such as a CD-ROM, floppy disk, or a computer memory, for instance a shared memory or shared disk on a networked computer system. Further still, the software product can be embodied in downloadable, and perhaps compressed and encrypted, computer data files that are later loaded and executed (or interpreted) by a general purpose computer or an image capture device. According to one embodiment, the invention is completely represented by the spoof detection module software alone -- and can be sold as a stand-alone product augmenting or improving an existing image capture device and/or biometric matching module.

The sensor 916 is preferably a capacitive fingerprint sensor. It is further described with reference to FIG. 9B, to which we now turn.

FIG. 9B shows a diagram of a fingerprint imaging device 932. In normal operation, the fingerprint imaging device 932 uses techniques derived from Coulombs law to determine the location of ridges and valleys in a fingerprint surface 938. By modeling each sensing element 936 in the sensor chip 916 as one plate in a capacitor, the finger surface 938 (that is, the ridges and valleys) being the second plate in the capacitor, it is possible to measure a relative distance between the ridges and valleys to construct an electrical representation of the fingerprint. According to one embodiment, a passivation layer 924 is disposed over the sensing elements 936 to form the capacitor at the ridges.

Turning back to FIG. 9A, when the sensor 916 detects an applied object 918 and captures an image, the individual sensing elements 936 create an electrical representation 920 of the surface 938 of the skin. In an abstract form, the electrical representation may be modeled as the fingerprint 922, wherein particular minutiae are highlighted by boxes only for the purpose of illustration. What is captured, however, is more than simply data representative of ridges and valleys in a fingerprint; anomalies, or "noise" (as is mentioned above) in the image will inevitably occur. These anomalies are discarded by prior systems, but here they are used to computationally analyze the electrical representation 920 for indicia of a living finger.

FIG. 2 is a block diagram of an alternative embodiment of a fingerprint system 5 for implementing the processes described below. Fingerprint system 5, in one embodiment, includes a fingerprint sensor 10 coupled to a processor 6 via a communication line 9. Fingerprint sensor 10 is for capturing fingerprint images from an applied object (e.g. finger 16) and is described in detail below. Processor 6 may be any processor capable of executing a software program. For example, processor 6 may be a central processing unit (CPU) of a conventional personal computer having a monitor 7, keyboard 8 and other peripheral devices (not shown) such as a mouse, biomedical measurement devices, and/or other biometric devices coupled thereto. Communication line 9 can be a serial communication path, such as a universal serial bus, between a serial interface of processor 6 and fingerprint sensor 10.

AVERAGE INTENSITY TECHNIQUE

FIG. 1 is a flowchart of a process of determining whether a fingerprint is coming from a living finger by calculating and comparing the average intensity of each image in a sequence of captured images.

The process of determining whether a fingerprint is coming from a living finger starts in box 102. An image is captured from an applied object by a fingerprint sensor in step 104. The image can be captured using, for example, a solid state fingerprint sensor, such as a capacitive sensor described in U.S. Patent Nos. 6,016,355, entitled "Capacitive Fingerprint Sensor," and 6,049,620, entitled "Capacitive Fingerprint Sensor with Adjustable Gain," and U.S. Patent Application Serial No. 09/354,386, filed July 14, 1999, entitled "A method of Constructing an Ultra-Rugged Biometric I.C. Sensor," and PCT International Application Serial No. PCT/US00/19227, filed July 13, 2000, entitled "Ultra-Rugged I.C. Sensor and Method for Making the Same," which are all incorporated herein by reference in their entirety. Capacitive sensors, such as those described in the above-mentioned references are manufactured using conventional CMOS silicon fabrication technology and include an array of pixels, each pixel comprising a capacitive sensing element. An exemplary sensor has an array of 300x300 pixels. In another embodiment, the image can be captured by a radio frequency based sensor, the radio frequency based sensor detecting surface texture or depth differentials between one or more layers of skin. In still another embodiment, the sensor can be a thermal sensor. In yet another embodiment, the sensor can be a swipe type sensor. (It is noted that these sensor embodiments can be employed in any of the techniques described below.)

Because capacitive fingerprint sensors require a three-dimensional object, they do not accept a two-dimensional photographic copy of a fingerprint. In addition, in order for these sensors to capture a fingerprint, the finger or object presented to the sensor must have electrostatic characteristics similar to the skin on a living finger. In other words, the object must be conductive. By requiring such electrostatic characteristics, fingerprints from plastic or rubber molded fingers can be eliminated, as these materials are non-conductive. Of course, other types of fingerprint sensors, e.g., optical sensors and pressures sensors, can be used as well.

Typically, the system uses a raw fingerprint image captured by the sensor to perform the spoof detection methods described herein. It is typically the case that the types of properties described herein, when electrically reproduced by the sensor, are found not, strictly speaking, found in ridge and valley data reproduced by the sensor. Rather, the properties are found in anomalies in the expected (perfect) fingerprint image and/or in other "non-linearities" or disturbances in the image. Thus, it may be undesirable in most, but not all, circumstances to process the raw fingerprint image to reduce the noise and enhance the raw image.

While some tests described below may benefit from such image processing, others may not. (Of course, alternatively, in some embodiments, once it has been determined the sampled image is a living fingerprint (and not a spoof), it may then be desirable to further process the raw data.) So, by way of example, image processing and/or filtering techniques such as those described in U.S. Patent No. 6,049,620, incorporated herein by reference above, U.S. Patent Application Serial Nos. 08/971,455, filed November 17, 1997, entitled "Automatic Adjustment Processing for Sensor Devices," Serial No. 09/300,087, filed April 26, 1999, entitled "Method for Imaging Fingerprints and Concealing Latent Fingerprints," and Serial No. 09/560,702, filed April 27, 2000, entitled "Automatic Gain Amplifier," which are each incorporated herein by reference in their entirety, can be employed.

Measurement for each pixel in the image can be translated into an analog signal representing the intensity of the pixel. In one embodiment, the value of the intensity is represented by a grayscale of 0 to 255 or 8 bits, 0 being the lightest (white, no signal) and 255 being the darkest (black, strong signal).

In general, an image generated from the conductivity measurements of a capacitive fingerprint sensor exhibits darker and lighter areas. These areas represent various levels of conductivity measured at the capacitors. As the finger, which acts as one plate of the

capacitor, becomes more conductive from moisture within the skin and on the skin surface (from perspiration), the image gets stronger, meaning that the intensity at each pixel increases. Furthermore, the darker intensity emanates from pore locations along the ridges as sweat is generated at these pore locations. As a result, image quality changes over time and these changes are secondary effects of the above-described biological characteristics. Hence, a sequence of images that exhibits an increase in image intensity may be deemed to be coming from a living finger.

An average intensity is calculated for the captured image in step 106. In one embodiment, the average intensity is ON-pixel normalized. That is, the average intensity of a captured image is an average of the intensities of the pixels that exhibit signal strengths that are greater than an ON-pixel threshold amount. The ON-pixel threshold is important in picture processing for extracting objects from their background and in this case, extracting ridges and valleys from a fingerprint. There are techniques that are known in the image processing arts for selecting an adequate threshold of gray level. One such technique example is described by N. Otsu in "A Threshold Selection Method From Gray-Level Histograms," IEEE Trans. Systems, Man, and Cybernetics, Vol. SMC-9, No. 1, Jan. 1979, pp. 62-66, which is incorporated herein by reference. In one embodiment, the ON-pixel threshold is 10. Thus, a pixel having a signal strength of 10 (e.g. on a scale of 0 to 255) is considered to be an ON-pixel (e.g. a ridge pixel).

In one embodiment, the average intensity is calculated for the full image, which can consist of the entire sensor area, e.g. 300x300 pixels. In another embodiment, the average intensity is calculated based on a portion of the captured image, for example, approximately 1/3 to approximately 2/3 of the central portion of the captured image. Calculation based on a portion of the captured image can reduce computational complexity without losing significant data because the central portion of the image typically contains the majority of the fingerprint image data.

The system then determines whether the captured image is a first image (step 108). If the captured image is a first captured image, then the capture device waits for a predetermined period of time in step 109, prior to capturing another fingerprint image (step 104). The predetermined time period is the actual capture rate, or the time between the capturing of two images. In one embodiment, actual capture rate is approximately 0.2 seconds. In general, actual capture rate depends on the capture device's capture rate (which

may be limited due to a particular physical or electrical configuration). The actual capture rate should give sufficient time for a detectable change in the level of the average intensity.

If the currently captured image is not the first image (step 108), then a delta average intensity is calculated from the average intensities of the currently captured image and the previous captured image in step 110. The delta average intensity between each two successively captured images is calculated by subtracting the average intensity of the previous captured image from the average intensity of the currently captured image.

In the embodiment shown in FIG. 1, the delta average intensity is calculated as each image is captured, on an image-by-image basis. In an alternative embodiment, the delta average intensity between each two successively captured images is calculated after a predetermined minimum number of images have been captured.

The system then determines whether the delta average intensity is positive in step 112. A counter that records the number of positive delta average intensities is incremented by one in step 114 if the delta average intensity is positive. The system then determines whether N1 images have been captured in step 116. Similarly, if the delta average intensity is not positive (step 112), then the system does not increment the counter but determines whether N1 images have been captured in step 116.

The value of number N1 depends on the rate of capture of the fingerprint sensor. According to one embodiment, using a capacitive fingerprint sensor, the minimum time for a sufficient change over the sequence of captured images is approximately 1.2 seconds. In this embodiment, at a capture rate of 0.2 seconds, six images are captured prior to any determination of whether the fingerprint is coming from a living finger. Similarly, if the capture device has a capture rate of, for example, 0.02 seconds per image, then a minimum of 60 images are captured prior to any determination.

If N1 images have not been captured (step 116), then an additional fingerprint image is captured in step 104 after a time delay (step 109). Steps 104 through steps 116 are repeated until N1 images have been captured.

After N1 images have been captured, an average delta average intensity is calculated in step 118. The average delta average intensity is calculated as (average of delta average intensities / average of average intensities). For example, for six average intensities (from six captured images) of 80, 90, 100, 110, 120 and 130, the average delta average intensity is calculated as:

$$[(10+10+10+10+10) / 5] / [(80+90+100+110+120+130) / 6] \times 100 \cong 9.5\%.$$

The system then determines whether the average intensity is increasing monotonically for the sequence of captured images (step 120). Monotonically increasing average intensity indicates that the applied object is warming up which is an indication of a living finger. A monotonically increasing average intensity is characterized by, for instance, 80% of the captured images having a positive delta average intensity.

An example is illustrative. If six images are captured, the same as in the above example, then the five delta average intensities are +10, +10, +10, +10, and +10. Since 100% of the images exhibit an increase in average intensity, the average intensity increases monotonically.

If the average intensity increases monotonically (step 120), then the system determines whether the average delta intensity is greater than a predetermined threshold amount (step 122). In one embodiment, the predetermined threshold is 10%. This value is selected based on experimentation. If the average delta intensity is greater than the predetermined threshold amount (step 122), then the image is accepted as coming from a living finger (step 124) and the process ends in step 126. All counters are reset at step 126. It is noted that steps 120 and 122 may be reversed in sequence or executed in parallel.

After N1 images have been captured, if the average intensity does not increase monotonically (step 120), or the average delta average intensity does not exceed the predetermined threshold amount (step 122), then a decision cannot be made as to whether the captured image is coming from a living finger or a spoof. When the decision cannot be made in the minimum time, e.g. 1.2 seconds for 6 images captured at a rate of 0.2 seconds, it is determined whether N2 images have been captured (step 128). N2 is the maximum number of images captured for the system to make a decision. If N2 images have not been captured (step 128), then an additional image is captured (step 104) after the time delay (step 109) until N2 images have been captured or until the system determines that the image is coming from a living finger. In one embodiment, the value of N2 is 15 (or the capture time is 3 seconds).

The average intensity of the additional image is calculated in step 106. The delta average intensity is calculated (step 110). The average delta average intensity is calculated (step 118). The system then determines whether the average intensity increases monotonically (step 120) and whether the average delta average intensity is greater than the threshold amount (step 122) as described above. If the average intensity increases

monotonically (step 120) and the average delta intensity is above a predetermined threshold amount (step 122), then the image is accepted as coming from a living finger (step 124).

If, however, the average intensity is not increasing monotonically or the average delta intensity is not greater the threshold amount and N2 images have been captured, then the image is rejected as coming from a spoof (step 130) and the process ends in step 126. In a static imaging environment, i.e. an environment where the applied object does not move relative to the sensor for image capture purposes, it is noted that the applied object, e.g. the finger, should remain on the fingerprint sensor until a decision is made. For example, the applied object must remain relatively stationary on the fingerprint sensor for a minimum of 1.2 seconds.

It is noted that in the embodiment above (FIG. 1), uniform sensor devices should be employed because different devices give different ranges of intensities. Since intensity ranges vary with different devices, it is difficult to use a fixed threshold while obtaining good or uniform results for all the devices. In addition, different fingers also give different ranges of intensities. Accordingly, the lack in uniformity causes it to be even more difficult to use a fixed threshold. Hence, where uniformity of the sensor is a concern, software and/or hardware based normalization may need to be performed on the sampled image(s) so that a different threshold does not need to be calculated for different people or different devices. Filtering and image processing techniques, such as those mentioned above for instance U.S. Patent Application Serial No. 09/560,702, filed April 27, 2000, as well as those discussed below, can be employed to achieve such a normalization.

PIXEL DENSITY TECHNIQUE

A more robust way of testing vitality is to use the density of ON-pixels along a ridge. Density is a measurement of the number of ON-pixels in a certain area, the certain area being the normalization factor. Because increased moisture within and on the surface of the skin increases the signals and that as the finger is warming up the sensor, the moisture increases, in particular, along the ridges. Hence, the ridge area is used in measuring the density of ON-pixels.

FIG. 3 shows a flowchart for determining whether a fingerprint is coming from a living finger by calculating the density of ON-pixels in a predetermined area. The process starts in step 150. A fingerprint image is captured in step 152. A portion of the captured image is selected in step 154. In one embodiment, a central portion of an image is selected.

For example, approximately 1/3 to approximately 2/3 of the central portion of the image is selected. In step 156, a maximum intensity value and a minimum intensity value for the pixels in the selected area are established. A mid-value between the maximum intensity value and the minimum intensity value is then determined in step 158. A pixel in the selected portion having an intensity value above the mid-value indicates an ON-pixel, or a ridge pixel (step 160). The ON-pixels in the selected portion are counted in step 162. Also in step 162, the density of the full image, or a portion thereof, is calculated by dividing the number of the ON-pixels into the total pixels in the selected portion.

The system then determines whether the captured image is the first image captured (step 164). If the captured image is the first image captured, then another fingerprint image is captured after a time delay (i.e. at a predetermined capture rate) in step 152. If the captured image is not the first image captured, then the change in density between the current captured image and the previous captured image is calculated in step 166.

The system then determines whether N3 images have been captured in step 168. Parameter N3 is the minimum number of images required prior to determining whether an image is coming from a living finger. If N3 images have not been captured, then another image is captured after a time delay (step 152). If N3 images have been captured, then the system determines whether the density increases monotonically in step 170. Similar to that described above, a counter counts the number of positive delta densities. If the number of positive delta densities exceeds a predetermined percentage, then the density of the sequence of images increase monotonically.

If the density does not increase monotonically, then the system checks whether N4 images have been captured in step 180. N4 is the maximum number of images captured for determining whether an image is coming from a living finger, similar to N2 described above. If the maximum number of images have not been captured, then another image is captured in step 152 after a time delay. If the maximum number of images have been captured, then the system rejects the image as coming from a spoof (step 182).

If the density increases monotonically, then the system calculates the average delta density (Step 172). Specifically, the delta densities are averaged and divided by the averaged density. If the average delta density exceeds a predetermined threshold amount (step 174), then the image is accepted as coming from a living finger (step 176) and the process ends in step 178. In one embodiment, the threshold amount is 0.35%.

If, however, the average delta density does not exceed the threshold, then it is determined whether N4 images have been captured (step 180). If less than N4 images have been captured, then an additional fingerprint image is capture in step 152 after a time delay. It is noted that all counters are reset in end step 178.

In one embodiment, to protect the system from falsely accepting an artificially warmed spoof, e.g. a spoof that is warmed by a hair blower, image characteristics are measured at different portions of the fingerprint. For instance, measurements can be taken from the middle of the fingerprint (middle fingerprint portion) and the outer peripheral of the fingerprint (outer fingerprint portion). The middle fingerprint portion typically warms up faster than the outer fingerprint portion for a living finger. To the contrary, the outer fingerprint portion of an artificially warmed spoof warms up faster than the middle fingerprint portion. Therefore, the system rejects the applied object as a spoof if the outer fingerprint portion warms up faster than the middle fingerprint portion.

In another embodiment, a predetermined portion of pixels is designated to be the middle fingerprint portion and the surrounding remaining area of pixels is designated as the outer fingerprint portion. For example, a center portion having 150x150 pixels is designated as the middle fingerprint portion and the surrounding remaining area of the 300x300 pixels is designated as the outer fingerprint portion. However, the number of pixels may be modified for different applications.

According to another embodiment, the average intensity is calculated for the middle fingerprint portion and the outer fingerprint portion of each image. The average intensity is calculated in a manner described above with respect to FIG. 1. Specifically, the intensity of the ON-pixels of an image are averaged. The rates of increase, i.e. the average delta average intensity, for the middle fingerprint portion and the outer fingerprint portion, are also calculated for each image. The rates of increase for the middle fingerprint portion and the rate of increase for the outer fingerprint portion are then compared. If the outer fingerprint portion has a rate that is greater than the rate for the middle fingerprint portion, then the system rejects the fingerprint as coming from a spoof. On the other hand, if the middle fingerprint portion has a rate of increase that is greater than the outer fingerprint portion, then the system accepts the fingerprint as coming from a living finger.

In an alternative embodiment, density is calculated for the middle fingerprint portion and the outer fingerprint portion of each image. The density is calculated in a manner described above with respect to FIG. 3. In one embodiment, ON-pixels in a center portion of

the image and along the ridges are counted and the density of ON-pixels is then calculated. ON-pixels in an outer portion surrounding the central portion of the image are also counted and the density calculated for each image. The rates of density increase for the middle fingerprint portion and the outer fingerprint portion are also calculated for each image. The rates of increase for the middle fingerprint portion and the rate of increase for the outer fingerprint portion are then compared. If the outer fingerprint portion has a rate that is greater than the rate for the middle fingerprint portion, then the system rejects the fingerprint as coming from a spoof. On the other hand, if the middle fingerprint portion has a rate of increase that is greater than the outer fingerprint portion, then the system accepts the fingerprint as coming from a living finger.

RATE OF WARMING TECHNIQUE

Another way to protect the system from falsely accepting an artificially warmed spoof is to measure the rate of warming due to the applied object and compare it to the rate of warming measured at the time of enrollment or during the subsequent successful verifications for the same finger. The rate of warming, in one embodiment, is calculated using average intensity. For example, average intensity of each captured image is calculated. A successive comparison of the average intensity is done for a currently captured image with the average intensity for a previous captured image. An average delta average intensity representing the rate of warming is then calculated. This rate is then compared with a rate of warming stored in a memory in the system. If the difference between the two rates exceeds a predetermined tolerance, then the system rejects the applied object as a spoof.

In an alternative embodiment, the rate of warming is calculated using density. For example, density of each captured image is calculated. A successive comparison of the density is performed for the density of a currently captured image with the density of a previous captured image. An average delta density representing the rate of warming is then calculated. This rate is then compared with a rate of warming stored in a memory in the system. If the difference between the two exceeds a predetermined tolerance, then the system rejects the applied object as a spoof. Comparing the rate of warming for an applied object and a previously determined rate of warming prevents false acceptance of an artificially warmed spoof because the warming characteristics of a spoof are different than the warming characteristics of a living finger.

RIDGE UNIFORMITY TECHNIQUE

FIG. 4 shows a flowchart for a process where the characteristic associated with perspiration is used to determine whether a fingerprint is from a living finger or a spoof by measuring the changes in intensity along the ridges over a sequence of images. The process starts in step 202. A plurality of images are sequentially captured at a predetermined rate, as is described above (step 204). The intensity along the ridges of each image is measured in step 206. The ridges are again represented by ON-pixels, the ON-pixels being the pixels that have intensities greater than a predetermined threshold.

The intensity along the ridges of each image is compared with intensity along corresponding ridges of a previous captured image successively (step 208). For example, the intensity along ridges of the second image is compared with corresponding intensity along ridges of the first image; the intensity along ridges of the third image is compared with corresponding intensity along ridges of the second image; and so on. If the intensity along the ridges increases in a spatially non-uniform way (step 210), then the system accepts the image as coming from a live person in step 212. This is because a spatially non-uniform increase in intensity along the ridges indicates pores emanating sweat, which is an indicator of a living finger. However, if the intensity along the ridges does not increase in a spatially non-uniform way (step 210), then the image is rejected as coming from a spoof in step 216. The process ends in step 214.

In an alternative embodiment, instead of global measurement of nonuniformly increasing intensity, the nonuniformly increasing intensity is measured along the contours of the ridges to obtain a linear sequence of intensity values. The contours are located by first determining the location of the ridges. The ridges are in turn determined by pixels having intensity values greater than a threshold amount. Pixels having intensities greater than a threshold amount are ON-pixels, as is described above. The image is then binarized, i.e. the ON-pixels are set as black pixels and the rest are set as white pixels. After binarization, the ridge measurement is linear.

A ridge follower (i.e. a computer technique that traces a line through analysis of a string of coterminous pixels) then tracks the ridges on the grayscale image, for example the original image prior to thresholding and binarizing. When the ridge follower is over a pore, the image signal is stronger and the image signal decreases after the ridge follower passed the pore. The signal level tracking a ridge is thus roughly sinusoidal as the signal goes from pore to pore. This nonuniformity in image signals does not exist for a dead or a fake finger

because they do not have pores. Therefore, the nonuniformity of signals of a ridge indicates vitality. The intensity periodicity and nonuniformity such as frequency may be measured, for example, by Fourier transform.

RIDGE SIGNAL STRENGTH TECHNIQUE

FIG. 5 shows a flowchart for a method of determining whether a fingerprint image is coming from a living finger by determining whether a ridge has maximum signal and the signal does not change. The method starts at box 302 and continues to step 304. In step 304, a sequence of images is captured. The images are compared successively in step 306, using either average intensity or density. If the average intensity or the density of the image does monotonically increase (step 308) and the ridge signals are strong (indicating that the signal is near a maximum value) (step 310), then the system accepts the image as coming from a living finger. In this case, the living finger may be a living finger that is wetted, or a living finger that is saturated due to perspiration caused by heat, exercise, etc. It is noted that a spoof is able to produce a strong signal and may be accepted falsely.

In another embodiment, depending on the security provisions, the system may prompt the user to wipe his finger and try again before accepting the image. In an alternative embodiment, the system may accept the fingerprint without further investigation (e.g. in a lower security application).

If the comparison in step 306 yields a result that the signals between images have changed (step 308), for example the difference is greater than a threshold value, then the system cannot determine whether the image is coming from a living finger (step 316). Similarly, if the signals indicate no change between images and the image does not have a maximum signal value -- i.e., the image strength is as high as the image capture device can measure --, then the system cannot determine whether the image is coming from a living finger (step 316) and the process terminates. The process terminates at box 314.

In one embodiment, instead of ending the process the system continues to look for other characteristics that are indicative of a living finger, such as checking the average intensity as described above in FIG. 1 and/or checking the uniformity of intensity along the ridges over a sequence of images, as described above with reference to FIG. 4.

In sum, the overall objective of the technique is to recognize certain limitations in image capture devices, or image capture means. For instance, due to limitations in the device, there will be circumstances where the initial image has as high a signal strength as the

device can measure. When this occurs, there is little ability to determine whether the change in image strength over a sequence of images gets stronger, which is a characteristic of a living finger. Accordingly, in one embodiment, gain adjustment techniques, such as those described in U.S. Patent Application Serial No. 09/560,702, filed April 27, 2000, incorporated herein by reference in its entirety above, can be employed when the signal strength is too high -- the gain adjustment technique can lower the image capture device gain and correspondingly lower the strength of the captured images so that a change is detectable. An alternative technique is to measure the signal strength along the middle of the ridges, which is described below in further detail.

WATER DROPLET DIFFERENTIAL TECHNIQUE

FIG. 6 is a flowchart depicting a situation where randomly located water droplets are used to determine whether the fingerprint is coming from a living finger or a spoof. The process starts in box 402 and continues to step 404. In step 404, a sequence of fingerprint images are captured. In step 406, randomly located, i.e. not all located along the ridges, water droplets are identified. Water droplets are indicated by splotches (e.g. globules) -- in this case clusters of pixels in the electrical representation that are representative of a splotch. Because water (at least perspiration) is conductive, water produces a strong signal. The system determines a globule if the ON-pixel area is wider than a ridge (a ridge is usually narrow and long versus a globule that has a larger width). If there is a large number of water droplets, then the applied object is likely either a wetted living finger or a wetted spoof.

The average size of the water droplets of a currently captured image is compared with corresponding water droplets in a previously captured image in step 408. If the water droplet size increases (step 410), then the system accepts the image as coming from a living finger (step 416) and the process ends in step 414. This is because, in general, a perspiring sweat gland creates moisture at a faster rate than the rate at which the skin absorbs the moisture. Hence, for a living finger, the water droplet size increases over time.

If the water droplet size remains static, or decreases over the timed sequence of images (step 410), or is too large, e.g. greater than approximately two or three ridge widths, then two situations may be possible: 1) the applied object is a wetted spoof or 2) the applied object is a living finger with over-accumulation of surface moisture. In either situation, the system does not accept the image as coming from a living finger (step 414), although the system may be falsely rejecting a living finger (as in the second situation).

In one embodiment, the system notifies the user to remove excessive moisture from the finger, e.g. by wiping the finger, and try again. When the user removes excess moisture from a true finger, the fingerprint will pass under the tests of FIGS. 1, 3, 4 and 5. A spoof, on the other hand, will either continue to fail under the test of FIG. 6 or, if the excessive moisture is removed from the spoof, then the fingerprint will then fail under the tests of FIGS. 1, 3, 4, 7 or 8.

FINGERPRINT VITALITY TECHNIQUE

FIG. 7 shows a flowchart for a method of distinguishing a living finger from a spoof by identifying the vitality of a fingerprint. The vitality is identified by processing a plurality of fingerprints captured over a predetermined period of time.

The process starts at box 502. In step 503 where a first fingerprint image is captured by a fingerprint sensor from an applied object at time zero. A last fingerprint image is captured after a predetermined (and programmable) time in step 504. According to an embodiment, the predetermined time is five seconds. In general, the predetermined time is selected to maximize the differences that can be observed between the captured images over the predetermined time frame. In an embodiment, a sequence of fingerprint images, e.g. nine images, are captured by a fingerprint sensor from the applied object during the predetermined time period. In another embodiment, only the first and the last captured images from the sequence of images are used for classification.

Image differences caused by temporal change in a perspiration pattern are used to determine whether the fingerprint is coming from a living finger or a spoof. More specifically, a living finger perspires, causing the signal pattern to change over time while changes due to perspiration do not occur in a dead or a fake finger. Hence, the finger should not be moisture-saturated when the first image is captured. In one embodiment, if the applied object gives a signal larger than a predetermined level, then the fingerprint verification system prompts the user to wipe his finger to eliminate excess moisture and try again.

Steps 506 through 512 describe a method for obtaining a mask from the last captured image. These steps are exemplary and other techniques can be employed.

The sequence of raw images are then processed through an image processing stage, including noise reduction, image enhancement and contour extraction in step 506, which can include any of the techniques described above, such as that described in U.S. Patent

Application Serial No. 09/560,702, filed April 27, 2000, entitled "Automatic Gain Amplifier," which is incorporated herein by reference above.

In one embodiment, a blank is captured from the fingerprint sensor, i.e. an image is captured from the fingerprint sensor without a finger placed on the sensor. This blank image represents the static in the background. A fingerprint is then captured from the fingerprint sensor and the blank image subtracted from the captured fingerprint to eliminate the static. In one embodiment, pixels that change within 2% of the blank image are discarded because they are considered to be static noise. In still other embodiments, a median filter can be applied to fill in the white pixels in the middle of the pores and to further smooth the image.

Also in step 506, the last captured image is translated into binary representation. The last captured image is used because a fingerprint from a living finger darkens over time due to increased moisture on the surface of the skin. Therefore, in general, the last captured image has the best contrast, meaning that it has the most defined ridge structure.

In another embodiment, the last captured image is first transformed into grayscale signals, represented by a number of 0 to 255. The last image is then transformed into binary representation by mapping pixels having signals greater than the threshold amount as a black pixel and a pixel having a signal less than a threshold amount as a white pixel.

Binarizing, according to one embodiment, is accomplished with a thresholding circuitry incorporated into the readout circuit of the sensor so that binary outputs are generated from the sense elements. The threshold can be set locally in specific regions of a fingerprint sensor to correct for variations across the sensor. A ridge is identified by the ON-pixels. A valley, on the other hand, is identified by the white pixels.

The binary image is then thinned so that ridges are only one pixel wide (step 508). Thinning reduces the amount of information to be processed to the minimum necessary for the recognition of patterns. In addition, the shape of a thin-line representation of a pattern is more easily analyzed, thus permitting a simpler structural analysis and more intuitive design of recognition algorithms. Preferably, a thinning algorithm compresses data representing the fingerprint, retain significant features of the pattern and eliminate local noise without introducing distortions of its own. Various thinning methods are described by L. Lam et al. in "Thinning Methodologies - A Comprehensive Survey," IEEE Trans. Pattern Analysis and Machine Intelligence, Sept. 1992, pp. 869-885. In general, any suitable method may be used to reduce the number of pixels to a curve of one pixel wide (i.e. a thin line).

In one embodiment, a shift is performed after thinning the binary image if the result does not pass through the middle of the original ridges. Shifting is performed because the main part of a ridge is more desirable than the borders of the ridge. The center of the ridges is preferred because the unique features, e.g. pores, of a living finger, reside in the center portion of the ridges rather than the borders of the ridges. Shifting involves moving the thinned line so that it corresponds to the middle of a thicker line from which it came. Preferably, a medial line, that is, one running down the middle of the thicker line, is desired. It is noted that, if thinning is accomplished by medial axis, then no such shifting is needed. The thinned line is moved from its current position so that it intersects midpoints of the thicker line. The midpoints can be determined by creating a line perpendicular to the thick line and identifying a middle point between the intersections of the boundaries of the perpendicular line across the thick line.

The y-connections are removed in step 510 so that the contours only consists of individual curves. A y-connection is where a ridge splits in two (i.e. bifurcates) and has multi-values (each leg of the y is defined by an equation, thus the joint has multiple values). In one embodiment, y-connections are removed by a simple 3x3 non-overlapping neighbor operation.

A 3x3 non-overlapping neighbor operation is useful not only in removing Y-connections, but filtering noise. The 3x3 non-overlapping neighbor operation applies a 3x3 pixel mask (or boundary) centered over a focal pixel (typically an ON-pixel). Thus, there exists a focal pixel and eight neighboring pixels. Next, the system examines each of the neighboring pixels. According to one embodiment, if no neighboring pixel is an ON-pixel, then the focal pixel is assumed to be noise. The process can be repeated for each pixel in the image. Furthermore, focal pixels with only one neighboring pixel that is an ON-pixel can be marked. The marked ON-pixel and focal pixel might, in fact, also be noise. So in a like manner, the marked ON-pixel can be processed as a new focal pixel and, if only one neighboring ON-pixel is found, then the marked ON-pixel and the original focal pixel are probably noise. Likewise, similar coterminous series of ON-pixels, of any desired length, can be eliminated in this manner. Of course, for circumstances greater than two pixel lengths, two neighboring ON-pixels, instead of one, would be the threshold criteria. Pixels assumed to be noise are turned off.

As for circumstances where a y-connection is to be removed, when a focal pixel (an ON-pixel) has two neighbors as ON-pixels, and the neighboring pixels are separated by, for

instance, at least one but not more than two, OFF-pixels, then it is possible that the series of three ON-pixels (the focal pixel and the two neighboring ON-pixels) represents a y-connection. In such a circumstance, the two neighboring ON-pixels are turned off.

After the image is thinned, the resulting contour representing each ridge includes the edge of each ridge (i.e. extremes). Extremes are undesirable because they are not a main part of the ridge but rather on the border of the ridge. As discussed before, the center portion of the ridge contains biological features that are unique to a living finger. Therefore, the end points on a contour (i.e. extremes) are eliminated. The spurs, which are tick marks along ridges (usually a one-bit or a two-bit intrusion), are eliminated as well.

In one embodiment, extremes of the ridges and the spurs are removed using 2-pixel erosion in step 512. A 2-pixel erosion can use the same basic 3x3 non-overlapping neighbor process. Here, a focal pixel has one neighbor. Thus, it is assumed that the focal pixel is an extreme or spur in a ridge. Consequently, the focal pixel is turned off. If extremes or ridges of greater than one pixel are to be removed, then the process can be performed in an iterative manner—once for each additional pixel of the extreme or spur to be removed.

In one embodiment, curves shorter than fifteen pixels are discarded (for instance, using the 3x3 non-overlapping neighbor process described above). Since the nominal pore-to-pore distance is approximately 0.5 mm, spanning approximately ten pixels, a curve shorter than fifteen pixels is too short to capture a pore and their vicinity adequately. At the end of this step, contours roughly follow the center of the ridges of the original captured image and largely contain useful information.

The results from the last captured image are used as a mask in step 514. The mask is placed over the first and the last captured images and the gray scales along the contours (i.e. the mask) of each of the first and last captured images are converted into signals (i.e. strings).

The resulting contours, which traverse through the middle of the ridges, have varying gray levels of the fingerprint image. It is noted that the peaks of the gray levels denote the moist (e.g. pore) locations and the valleys of the gray levels show the dryer regions, usually between each two pores. Typically, there is regularity in the spacing of the pores in a live fingerprint signal. For example, the peak to peak distance in a live fingerprint signal is approximately 10 pixels or 0.5 mm. This is opposed to a fingerprint signal from a dead finger or a plastic finger, which does not have a specific periodicity because a spoof does not have evenly spaced perspiring pores.

In step 528, the periodicity of gray levels on each string in the first captured image is measured by a Fourier transform. In one embodiment, the FFT (Fast Fourier Transform) is used because it reveals periodicities (e.g. relative variability) observed across different frequencies of an image. The first captured image is typically "patchy," meaning that when a dry finger is first placed on a fingerprint sensor, gray scale only shows up around the pore areas due to droplets of sweat forming around the pores and the rest of the ridges may not show clearly. Thus, a FFT is done for the first captured image to quantify the variability in gray level along the ridges due to the pores and the presence of perspiration.

A FFT is a known algorithm that is computationally much faster for large numbers of samples in the sequence. Any type of FFT algorithm can be used, for example, mixed radix method, radix 2 method, decimation in time method and the Danlielson-Lanczos Lemma method are all well known and readily available. In another embodiment, a 256-point FFT command is performed. In one embodiment, prior to taking the FFT, the DC signal is removed to eliminate a spike near zero frequency.

The patchiness of a fingerprint changes over time as the ridges become more uniform. This is because sweat emanating from a pore spreads and migrates to dryer parts of the finger. When the last image is taken after a time delay, gray scales typically show up all along the ridges due to moisture spreading towards drier parts of the finger. Thus, there is less variability and a FFT is not performed for the last captured image. Instead, the last captured image is used to extract temporal changes relative to the first capture, which is discussed below.

It is noted that if the finger is already saturated with moisture when the first image is captured, then the first image will not exhibit variability in gray scale. In addition, the last image captured after a time delay will not exhibit sufficient signal change from the first captured image if the finger is initially saturated with moisture. Hence, the finger should not be moisture-saturated when the first image is captured.

For a live fingerprint, the signal representing the first captured image exhibits periodic peaks and valleys having a particular spatial frequency for the peaks. The peaks correspond to pore locations. Also in step 528, the total energy that corresponds to the spatial frequency of the pores is calculated. In general, spatial frequency is defined in cycles/pixel or cycles/mm. The total energy is the approximation of the area under the signal curve that is a result of the FFT. All the numbers in a predetermined window that correspond to spatial distance of approximately 0.4 mm to approximately 1.2 mm are added up, the result of which

is the total energy. Spatial distances of 0.4 mm and 1.2 mm are selected, because as discussed above, the average pore-to-pore distance is approximately 0.5 mm. Assuming a ±0.1 mm variation, for example, the minimum spatial distance is approximately 0.4 mm. A pore may be missing, e.g. a pore that is not sweating. Therefore, the maximum distance between two sweating pores is approximately 1.2 mm.

As discussed before, because a spoof does not have pores, no spatial frequency is available for a spoof. Hence, the total energy for a spoof is of a negligible value, or much less than that of a living finger.

In parallel to step 528 are steps 516 through 526, where temporal changes of a fingerprint are quantified. In step 516, signals representing the contours are connected to form a long signal that represents each of the first captured fingerprint and the last captured fingerprint. The local maximums and local minimums of the first and the last fingerprint signals are detected in step 518. Local maximums are all the different peaks in the long signal and local minimums are all the different valleys in the long signal. Because the long signal exhibits periodic ups and downs, there are multiple peaks and valleys within one signal. This is opposed to a global maximum and a global minimum where only one peak and one valley is selected from the long signal.

The local maximum and the local minimum are used to calculate a series of parameters quantifying the changes caused by the sweating process over time. For live fingerprint signals, the local maximums are typically fairly constant, but the local minimums typically rise over time due to the diffusion of perspiration. In general, the pixels near the pores are relatively saturated while the areas between the pores are relatively dry when the first image is captured, creating fluctuation in the fingerprint signal. However, as time progresses and the sweat diffuses toward dryer regions, the signal becomes more homogeneous (and thus less varying gray level along the ridges). In one embodiment, the series of parameters include total swing ratio (step 520), minimum and maximum growth ratio (step 522), last-first fingerprint signal difference (step 524) and percent change of standard deviation of the first and the last fingerprint signal (step 526). These four parameters are chosen because these four parameters exhibit sufficient differences between a dead and a live fingerprint signal.

In step 520, the total swing ratio of the first fingerprint signal to the last fingerprint signal is calculated. In general, the swing for a live fingerprint is larger than that of a spoof (a fake or dead finger). In addition, the swing is generally smaller for the last captured image

as compared to the first captured image. As discussed above, moisture begins mainly around the pores creating peaks in the signal. As the time progresses, the moisture gradually spreads along the ridges. Thus, the total swing decreases over time. Because a spoof does not have perspiring pores, this general trend is not present for a spoof fingerprint signal.

Total swing ratio of first captured fingerprint signal to the last captured fingerprint signal is calculated as follows:

$$D.M.1 = \Sigma |(C_{1\,i} - C_{1\,i-1})| \,/\, \Sigma |(C_{2\,i} - C_{2\,i-1})| \qquad (1)$$

where C_i is the intensity value of the image at point i along the contour, C_1 denotes the first capture; C_2 denotes the last capture, and the sum is taken for all i=2, 3, ..., C_2 length. It is noted that length C_1 is equal to length C_2 because both the first and the last captured images use the same mask.

In step 522, minimum/maximum growth ratio of first to last fingerprint signal is calculated. As discussed above, for a live fingerprint signal, the height of the local maximums (peaks) increases at a slower rate than the height of the local minimums (valleys). Therefore, the average ratio of the local minimum growth to the local maximum growth is typically larger for a live fingerprint signal as compared to a spoof fingerprint signal. The minimum/maximum growth ratio of first to last fingerprint signal is calculated using the following equation.

$$D.M.2 = \Sigma(C_2^{min}{}_j - C_1^{min}{}_j) \,/\, \Sigma(C_2^{max}{}_i - C_1^{max}{}_i), \qquad (2)$$

where i and j are the maximum/minimum location indexes extracted from the second capture C_2 (the first capture C_1 maximums/minimums are read from the same locations accordingly.)

In step 524, the last-first fingerprint signal difference mean is calculated. Because a nonliving finger does not perspire, the last captured fingerprint signal subtracts the first captured fingerprint signal exhibits a lower degree of change than the signal difference between the first captured fingerprint signal and the last captured fingerprint signal for a living finger. The last-first fingerprint signal difference mean is calculated as follows.

$$D.M.3 = (\Sigma(C_{2\,i} - C_{1\,i})) \,/\, n,\ i = 1, 2, ..., n \qquad (3)$$

where n = length C_2 = length C_1.

Percentage change of standard deviations of first and last fingerprint signals is calculated in step 526 as follows.

$$D.M.4 = (SD(C_1) - SD(C_2) \,/\, SD(C_1)) \qquad (4)$$

where SD is Standard Deviation Operator: $SD(X) = (\Sigma(x_i - mean(x))^2 \,/\, (n-1))^{1/2}$, n = length X.

If the signal fluctuation decreases around the means, which is typical for a live fingerprint signal, then the percentage change of standard deviation would rise. Hence, a higher value of percentage change of standard deviations of the first and the last fingerprint signals indicates a living finger.

The results from steps 520 through 528 are then fed into a back-propagation neural network classifier. In step 530, a decision on vitality is made in accordance to the results from the back-propagation neural network classifier. It is noted that the back-propagation neural network classifier can classify a fingerprint signal based on any one of these five measurements. However, a combination with one or more other measurements can produce better classification precision and thus a more robust system than using one measurement alone.

A neural network is a software (or hardware) simulation of a biological brain. One advantage a neural network has over digital computers is the ease of taking into account high-order statistical relationships of stochastic data. More specifically, a neural network learns to recognize patterns in an input data by utilizing the principle of reward and punishment, by back-propagating the needed information for altering structures of interconnections and strength or weights of these interconnections dynamically. Once the neural network has been trained on samples of input data, it can make predictions by detecting similar patterns in future data.

The architecture of a back-propagation neural network consists of two major components: nodes and the connections between the nodes. The back-propagation neural network is a multi-layered network, with the output from one layer serving as input to the next. The layers with no external output connections are referred to as hidden layers. A back-propagation network with a single hidden layer consists of three layers of nodes (input, hidden, and output) and full interconnection between input and hidden layers and the hidden and output layers. Residing on these connections are weights that multiply signals passing over the connection. The product of the signal magnitude and weight is summed over all connections leading to a particular node to give the initial output for that neuron (the actual result is dictated by the activation function chosen for the node). In general, the number of hidden layer neurons should be approximately one-half of the input layer nodes.

Training begins with all weights set to random numbers. For each data record, the predicted value is compared to the desired (actual) value and the weights are adjusted to move the prediction closer to the desired value. Many cycles are made through the entire set

of training data with the weights being continually adjusted to produce more accurate predictions. In one embodiment, a back-propagation neural net (three layer perceptron), with sigmoid non-linearity, is used.

Training a neural network requires the use of the same parameters that will be used to make the classification. Training involves, for example, different data sets of the five parameters from subjects in each classification. For instance, one classification may be a living finger, one classification may be a dead finger, and one classification may be a plastic finger. In another instance, twelve data sets are collected from each class. According to one embodiment, the training algorithm uses gradient descent in conjunction to batch input-output training vectors to classify the input cases as live or spoof. In another embodiment, bipolar targets (+1, -1) are chosen to denote live and spoof, respectively.

If the output of the back-propagation neural network indicates that the fingerprint is from a living finger (step 532), then the system passes the fingerprint as coming from a living finger (step 540) and the process ends in step 544. However, if the output of the back-propagation neural network indicates that the fingerprint is from a spoof (step 532), then it is determined whether the number of trials is equal to a predetermined number, e.g. 3 (step 534).

If the number of trials has reached the predetermined number, then the system indicates that the fingerprint failed and cannot be accepted as coming from a live person (step 542). The process ends in step 544. It is noted that each time input data travels through the back-propagation neural network, a counter recording the number of trials is incremented by one. The counter is reset at the end step 544.

If the number of trials has not reached the predetermined number, then the system prompts the user to wipe his finger and try again in step 536. The process repeats by returning to the start step (step 538).

INVERTED SPOOF DETECTION TECHNIQUES

Turning to FIG. 8, it depicts a method for distinguishing between a real fingerprint and an inverted spoof of the fingerprint. An inverted spoof is created when the ridge and valleys of an enrolled fingerprint are essentially turned inside-out. The inverted spoof is a fairly simple technique for fooling a fingerprint capture system. Indeed, it can be particularly powerful: turning contour of the finger inside-out maintains the ridges and valleys -- or at

least their transition points (endpoints and bifurcations), which is what is compared according to an embodiment of the system.

In order to detect an inverted fingerprint, characteristics of the transition points are analyzed and compared between the enrolled fingerprint data and the captured fingerprint data. More particularly, and in the embodiment described below, when a fingerprint contour is inverted, the bifurcations become endpoints and vise-versa; the system, accordingly, performs a statistical analysis on the ratio of bifurcations to endpoints, with respect to matching minutiae, to detect the inversion.

In step 804, the fingerprint sensor captures an image of the applied object (the finger). In step 808, minutiae are compared between the captured image and an enrolled image. A test is performed in step 812 to determine whether a match was found in step 808. If a match was found then, in step 816, a match counter is incremented (once for each match if multiple minutia are compared in step 808).

In step 820, the matching minutiae are classified by type by extracting information from the image. By classifying each minutia by type it is meant is endpoints and bifurcations are so marked. If the matching minutiae of the enrolled image have not already been classified, then they are classified too. According to one embodiment, to classify the minutiae by type, the 3x3 non-overlapping neighbor technique, described above, can be employed. Y-connections (bifurcations) can be extracted by examining at least three ON-pixels in the proximity of the minutia, while endpoints can be extracted by examining at least two ON-pixels in the proximity of the minutia. If the image has been filtered, in accordance with the process described above with reference to FIG. 7, then such information can be extracted then, rather than in a separate step as is depicted in FIG. 7.

In step 824, a test is performed to determine whether the captured and enrolled minutiae are of the same type. If they are not, then a type mismatch counter is incremented in step 828. If they are, or after step 828, then a next test (step 832) determines whether there are more minutia that need to be compared. If there are more minutiae to be compared, then a next minutiae is retried in step 836 and processing continues to step 808. If there are no more minutiae to be compared, then in step 840 the ratio of the type mismatch counter value to the match counter value is calculated.

A test is performed in step 844 to determine whether the calculated ratio exceeds a threshold value. According to one embodiment, the threshold value is 50%. This is because the inventors have found that due to potential non-uniformities in, for instance, a capacitive

fingerprint sensor, and/or environmental conditions, a number minutiae will be misclassified -- in particular where pixel intensity at or near an endpoint or bifurcation is just below the ON-pixel threshold value. The threshold value, can however, be reduced to a much lower tolerance if proper filtering or more ideal environmental conditions are present.

If the ratio exceeds the threshold, then in step 848 the captured image is rejected as an inverted spoof. Otherwise, in step 852, the captured image is identified as not being an inverted spoof and the captured image is either accepted, or other security constrains enforced.

ADDITIONAL TECHNIQUES

Additional tests may be executed to deal with varying environmental conditions. In one embodiment, the rate of effects under different environmental conditions is compared with the rate of effects under ambient conditions, such as temperature and humidity, for adjustment of certain predetermined parameters. For example, the rate of heating in freezing temperature and the rate of heating in extreme heat differ from the rate of heating under ambient temperature. Another example is that the rate of heating in dry weather and the rate of heating in humid weather differ from the rate of heating under ambient condition. Because the rate of heating varies under different environmental conditions, the minimum time and the maximum time for determining whether a fingerprint is coming from a living finger, for example, are modified according to the ambient conditions. For example, in cold weather, instead of a minimum time of 1.2 seconds, the system waits for 3 seconds and instead of a maximum time of 3 seconds, the system allows for 5 seconds to determine whether the finger is alive.

In one embodiment, pore placement is measured along the ridges to detect whether the pore pattern matches that of the true enrolled finger or a previously successfully verified finger. Pore placement can be measured directly or by locations of the sweat droplets as described above. More specifically, in one embodiment, pores are detected by detecting the peaks of a sinusoidal curve. Since the pores are very shallow and small, their fine features are not easily replicated by a spoof. Hence, pore placement may be a test for a true, versus a fake, finger.

In another embodiment, a global measurement of the texture of a finger is performed and the result compared with the texture of a finger measured during enrollment or measured during a previous successful verification. The skin of a living finger has very fine features

that cannot be easily reconstituted in a rendition of that finger. These fine features may be, for instance, measured and quantified by using Fourier transform and looking at the high frequency details. A living finger, in general, has higher frequency details then a plastic finger. The texture measured may be, but not limited to, pores and other small texture that cannot be readily and reliably reproduced. In one embodiment, the textures may be measured using a device that measures very fine features.

According to another embodiment, a biomedical measurement device is used to measure certain characteristics of a living finger, such as, but not limited to, skin resistance, temperature, pulse-oximetry (blood oxygen measured by absorption of near infrared light and red light), electrocardiogram (electrical potential changes of cardiac activity versus time), laser Doppler measurement of blood flow, x-ray, pressure and other physiological vitality indicators. These measurements are compared with corresponding measurements taken during enrollment or during a previous successful verification.

In still another embodiment, the system is a multi-modal system which requires more than one biometric measurements such as, but are not limited to, fingerprint, voice, hand-writing, retina, etc. By using a multi-modal system, an attacker must obtain multiple tools to manufacture different modes of spoof, thus making a spoof attack more difficult.

According to another embodiment, the system requests a user to put the same finger down on the capture device twice. A sequence of images is captured for each application. The first and the second sequence of images are then compared. It is noted that the fingerprint images from a living finger exhibit some hysteresis as the characteristics change. In particular, the first of the second sequence of images exhibits characteristics closer to the last image of the first sequence of images. The first image of the second sequence of images from a spoof, on the other hand, displays characteristics that are closer to the first image of the first sequence of images captured from the initial application. This difference is due to the fact that a finger has an elastic surface, thus the surface of the finger stretches and varies under different conditions. Hence, the closer in time the fingerprints are taken, the closer the images. In contrast, a molded finger typically produces identical fingerprints during initial application. Therefore, by comparing the images from two different applications, the system is able to determine whether the applied object is a living finger.

Although the invention has been described with reference to particular embodiments, the description is only an example of the invention's application and should not be taken as a

limitation. For example, other types of classifier may be used to classify the fingerprint signals. For instance, a classifier may be devised using the median values derived from a training set to determine a threshold. The classifier may than accept or reject a fingerprint signal based on the threshold value. Various other adaptations and combinations of features of the embodiments disclosed are within the scope of the invention as defined by the following claims.

In one embodiment, the system can include an algorithm that randomly selects and requests one or more fingers for measurements, the maximum allowable number of fingers requested being ten. Randomly requesting different and varying number of fingers makes the attack more difficult because it is more difficult for an attacker to manufacture multiple spoofs. Furthermore, any of the particular spoof detection techniques described above can also employed, on a case-by-case basis, to detect a spoof. Since the selection of the finger and/or algorithm is random, it adds unpredictability (with respect to potential spoofers), thus making the system more resistant to attacks.

CLAIMS

What is claimed is:

1. A biometric sensing system comprising:

an image capture device configured to sample an applied object and create an electrical representation of the applied object; and

a spoof detection module configured to analyze the electrical representation of the applied object for relative intensity, density, geometric, or temporal anomalies indicative of a non-living applied object.

2. The biometric sensing system of claim 1, wherein the spoof detection module employs an average intensity technique to detect and classify the anomalies, the average intensity technique configured to cause the system to capture a plurality of images of the applied object, and calculate an average intensity for each of the plurality of captured images.

3. The biometric sensing system of claim 2, wherein the average intensity technique is further configured to cause the system to reject the applied object as a spoof when the average intensity does not increase monotonically over the plurality of images.

4. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a pixel density technique to detect and classify the anomalies, the pixel density technique configured to cause the system to capture a plurality of images of the applied object, determine an ON-pixel value based upon a first captured image, determine a pixel count for each image in the plurality of captured images, wherein the counted pixels exceed the ON-pixel value, and calculate a delta pixel count value over the plurality of images.

5. The biometric sensing system of claim 4, wherein the pixel density technique is further configured to cause the system to reject the applied object as a spoof when the delta pixel count does not increase monotonically over the plurality of images.

6. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to capture a plurality of images of the

applied object, measure pixel intensity along ridges in each of the plurality of captured images, determine whether the pixel intensity increases in a spatially non-uniform manner, and reject the applied object as a spoof when the pixel intensity does not increase in the spatially non-uniform manner.

7. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to capture a plurality of images of the applied object, measure pixel intensity along ridges in each of the plurality of captured images, determine whether the pixel intensity increases in a spatially non-uniform manner, and reject the applied object as a spoof when the pixel intensity does not increase in the spatially non-uniform manner.

8. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to capture a plurality of images of the applied object, measure pixel intensity values along contours of ridges in each of the plurality of captured images, binarize the pixel intensity values, measure pixel intensity variations along the ridges, and reject the applied object as a spoof when the measured pixel intensity variations are not roughly sinusoidal.

9. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a water droplet differential technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to capture an image of an applied object, locate a first water droplet positioned within the image, capture a subsequent image of the applied object, locate a like-positioned water droplet within the subsequently captured image, compare a size of the first water droplet with a size of the like-positioned water droplet, and reject the applied object as a spoof when the size of the like-positioned water droplet is smaller than the size of the first water droplet.

10. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a fingerprint vitality technique to detect and classify the anomalies, the fingerprint vitality technique configured to cause the system to capture a plurality of images

of an applied object, digitally process the plurality of captured images, form a fingerprint signal representative of fingerprint strings from each of the plurality of images, compare changes between the fingerprint signal corresponding to an initial image in the plurality of images and a fingerprint signal from a subsequently captured image in the plurality of images, and reject the applied object as a spoof when the changes exceed a threshold amount.

11. The biometric sensing system of claim 10, wherein the fingerprint vitality technique is further configured to cause the system to compare a total swing ratio of the fingerprint signal of the initial image and the fingerprint signal of the subsequently captured image.

12. The biometric sensing system of claim 10 or 11, wherein the fingerprint vitality technique is further configured to cause the system to compare a minimum or a maximum growth ratio as between the fingerprint signal of the initial image and the fingerprint signal of the subsequently captured image.

13. The biometric sensing system of claim 10, 11 or 12, wherein the fingerprint vitality technique is further configured to cause the system to compare last to first fingerprint signal difference mean between the plurality of images.

14. The biometric sensing system of claim 10, 11, 12 or 13, wherein the fingerprint vitality technique is further configured to cause the system to compare a percentage change of standard deviations between the fingerprint signal of the initial image and the fingerprint signal of the subsequently captured image.

15. The biometric sensing system of claim 10-14 or 15, further comprising a neural network, wherein the neural network configured to perform the steps of comparing.

16. The biometric sensing system of any of the above claims, wherein the spoof detection module is configured to extract minutia type information from the electrical representation, compare minutia type information with information corresponding to an enrolled object, calculate a ratio of mismatched minutia type information to matching minutia information, and reject the applied object as an inverted spoof when the ratio exceeds a threshold type mismatch ratio.

17. The biometric sensing system of any of the above claims, further comprising a minutia matching module configured to compare minutiae extracted from the electrical representation of the applied object with minutiae of an enrolled object.

18. The biometric sensing system of any of the above claims, wherein the image capture device is a capacitive fingerprint sensor.

19. A computer implemented method for detecting a spoof of a living finger, comprising:

receiving one or more electrical representations representative of a plurality of images of an applied object; and

analyzing the one or more electrical representations for relative intensity, density, or geometric anomalies indicative of a non-living applied object.

20. The method of claim 19, wherein the step of analyzing comprises:

calculating an average intensity for each of the plurality of images; and

rejecting the applied object as a spoof when the average intensity, as sequentially measured over the plurality of images, does not increase monotonically.

21. The method of claim 20, further comprising:

calculating an average change in the average intensity of the plurality of images; and

rejecting the applied object as a spoof when the average change in the average intensity is below a threshold average change in the average intensity value.

22. The method of claim 19, 20 or 21, wherein the step of analyzing comprises:

selecting a portion of a first image in the plurality of images;

determining an ON-pixel value based upon intensity values in the portion of the first image;

counting a number of pixels exceeding the ON-pixel value in the portion of the first image;

repeating the above steps of selecting, determining, and counting for a next image in the plurality of images;

calculating an average density value between the first image and the next image; and

rejecting the applied object as a spoof when the average density value is not increasing monotonically.

23. The method of claim 22, further comprising:

calculating an average change in average density between the plurality of images; and

rejecting the applied object as a spoof when the average change in average density is less than a threshold average change in average density value.

24. The method of claim 19, 20, 21, 22 or 23, wherein the step of analyzing comprises:

measuring intensity along ridges in each of the plurality of images;

comparing the intensity along the ridges from each captured image with the intensity along the ridges from a coterminously captured image;

determining whether the intensity along the ridges increases in a spatially non-uniform manner; and

rejecting the applied object as a spoof when the intensity along the ridges does not increase in a spatially non-uniform manner.

25. The method of claim 19, 20, 21, 22, 23 or 24, wherein the step of analyzing comprises:

comparing the electrical representations of each of the plurality of images for changes;

comparing maximum signal values in the electrical representations when there are insignificant changes between the electrical representations;

rejecting the applied object as a spoof when the electrical representation holds signal values indicative of insignificant changes between successive images.

26. The method of claim 19, 20, 21, 22, 23, 24 or 25, wherein the step of analyzing comprises:

locating water droplets in each of the plurality of images;

comparing a size of the water droplet in each of the plurality of images with a size of the water droplet in a subsequently captured image in the plurality of images;

rejecting the applied object as a spoof when the water droplet size is static or decreases, over time, as represented in the plurality of images.

27. The method of claim 19, 20, 21, 22, 23, 24, 25 or 26, wherein the step of analyzing comprises:

digitally processing a first electrical representation;

saving the digitally processed electrical representation as a mask;

applying the mask over subsequent electrical representations;

converting the result of the mask of the subsequent electrical representations into fingerprint strings;

connecting the fingerprint strings into a fingerprint signal for each image;

analyzing the fingerprint signal for anomalies; and

rejecting the fingerprint signal when the anomalies are not indicative of a living finger.

28. The method of claim 27,

wherein analyzing the fingerprint signal for anomalies comprises calculating a total swing ratio of a first fingerprint signal to a last fingerprint signal; and

rejecting the fingerprint signal when the total swing ratio is not indicative of a living finger.

29. The method of claim 27 or 28,

wherein analyzing the fingerprint signal for anomalies comprises: calculating a minimum or maximum growth ratio as measured between a first fingerprint signal and a last fingerprint signal; and

rejecting the fingerprint signal when the growth ratio is not indicative of a living finger.

30. The method of claim 27, 28 or 29,

wherein analyzing the fingerprint signal for anomalies comprises calculating a first fingerprint signal to a last fingerprint signal difference mean; and

rejecting the fingerprint signal when the signal difference mean is not indicative of a living finger.

31. The method of claim 27, 28, 29 or 30,

wherein analyzing the fingerprint signal for anomalies comprises calculating a percentage change of standard deviation between a first fingerprint signal and a last fingerprint signal; and

rejecting the fingerprint signal when the signal difference mean is not indicative of a living finger.

32. The method of claim 27, 28, 29, 30 or 31, further comprising:

calculating a spatial frequency of peaks in the fingerprint strings;

calculating a total energy for the fingerprint strings, based on the spatial frequency; and

rejecting the fingerprint signal as a spoof when the average energy is below a threshold total energy.

33. The method of claim 27, 28, 29, 30, 31 or 32, further comprising, prior to rejecting the fingerprint signal as a spoof, sending the anomalies to a neural network for classification.

34. The method of claim 19-32 or 33, wherein the step of analyzing the one or more electrical representations comprises:

extracting minutia type information from the electrical representation;

determining whether the minutia type information matches a minutia type of a matching minutia from an enrolled finger;

calculating a ratio of mismatched minutia types to matching minutia; and

rejecting the fingerprint signal as a spoof when the ratio of mismatched minutia types to matching minutia exceeds a threshold mismatch value.

35. The method of claim 19-33, or 34, further comprising:

capturing the plurality of images of the applied object with a fingerprint sensor; and

converting the plurality of images into the one or more electrical representations of the applied object.

36. The method of claim 35, wherein the fingerprint sensor captured the plurality of images with a capacitive fingerprint sensor.

37. The method of claim 19-35, or 36, further comprising matching minutiae extracted from at the one or more electrical representations with minutiae from an enrolled finger.

38. A computer software product having stored therein one or more sequences of instructions for causing one or more processors to perform any of steps as recited in any of above claims 19 through 37.

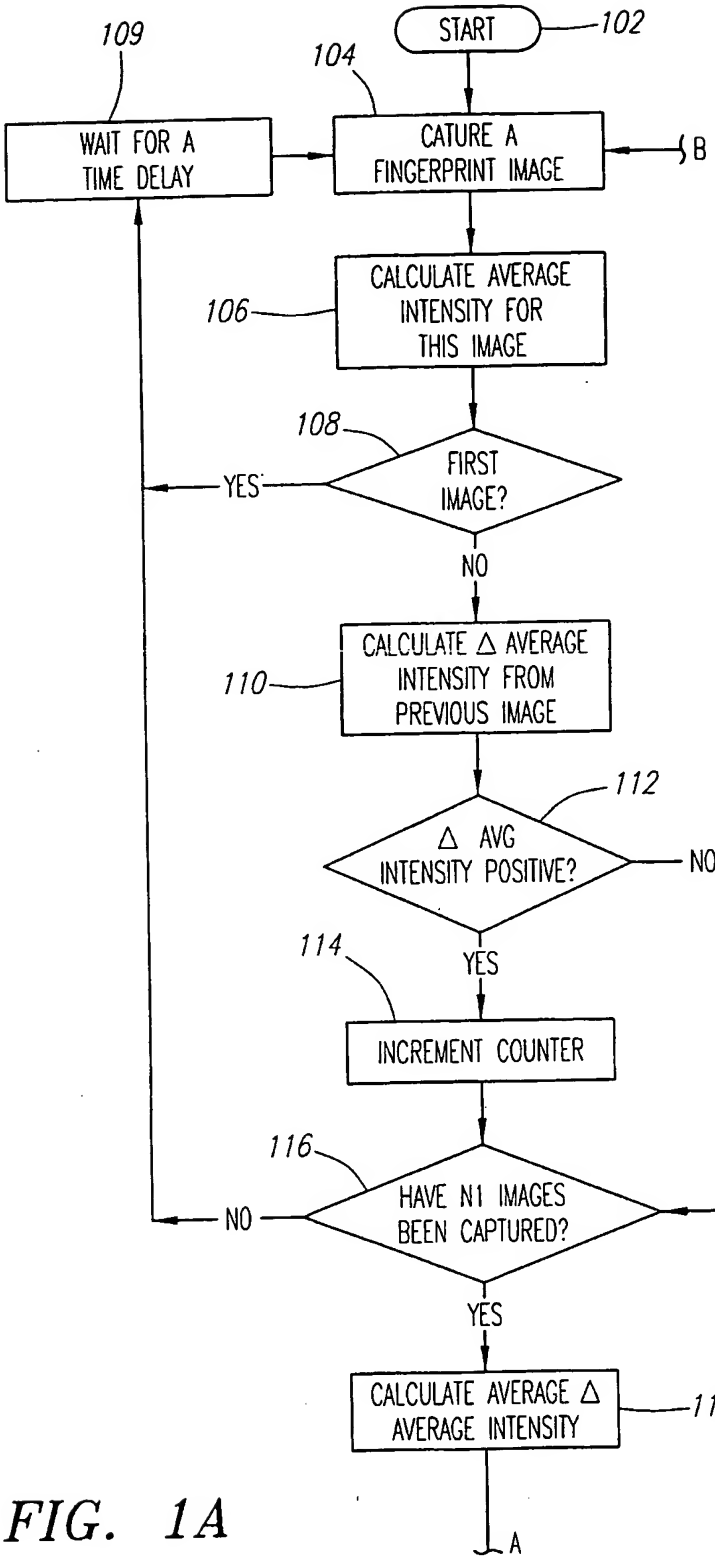


FIG. 1A

FIG. 1A
FIG. 1B

FIG. 1

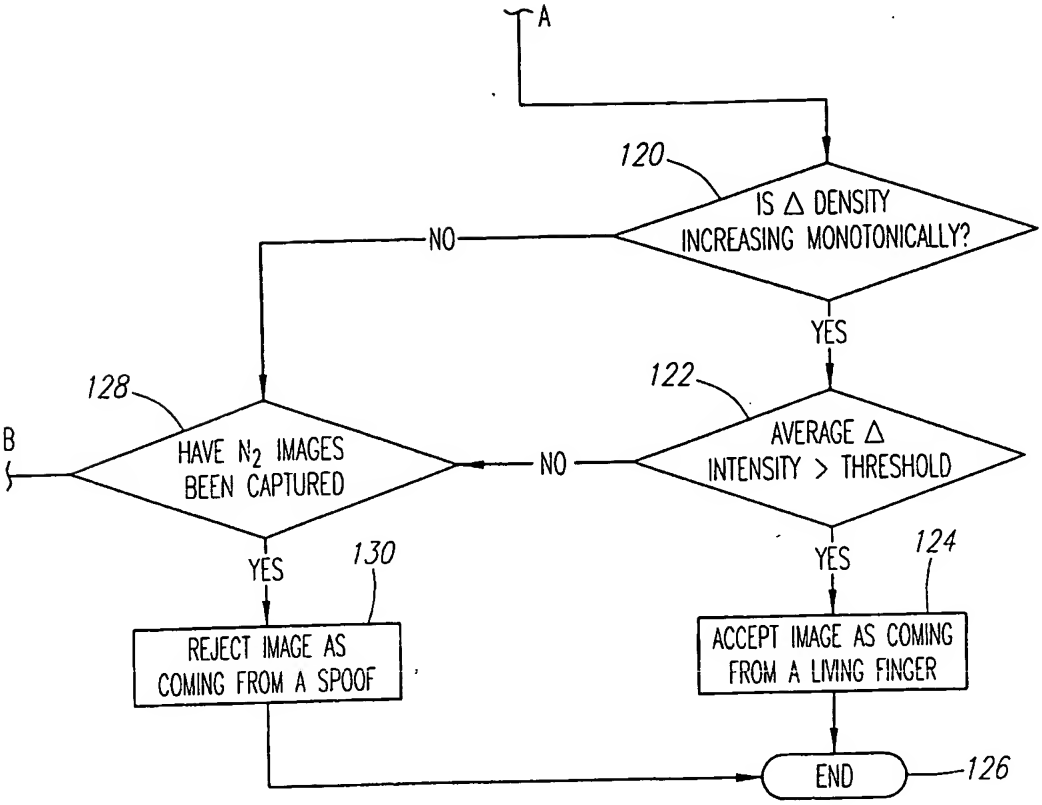

A
120
IS Δ DENSITY INCREASING MONOTONICALLY?
NO
YES
128
122
B
HAVE N_2 IMAGES BEEN CAPTURED
NO
AVERAGE Δ INTENSITY > THRESHOLD
YES
130
YES
124
REJECT IMAGE AS COMING FROM A SPOOF
ACCEPT IMAGE AS COMING FROM A LIVING FINGER
END
126

FIG. 1B

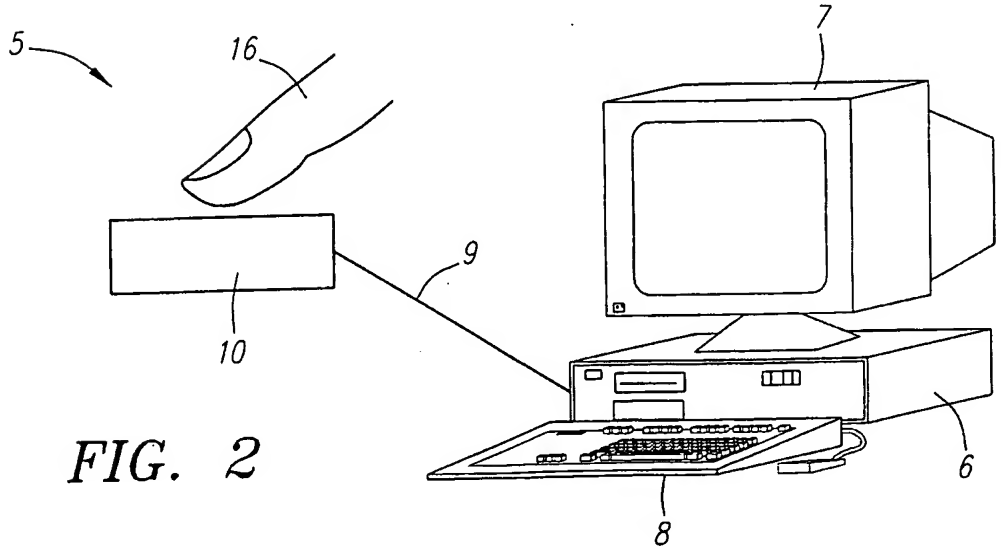

5
16
7
9
10
6
8

FIG. 2

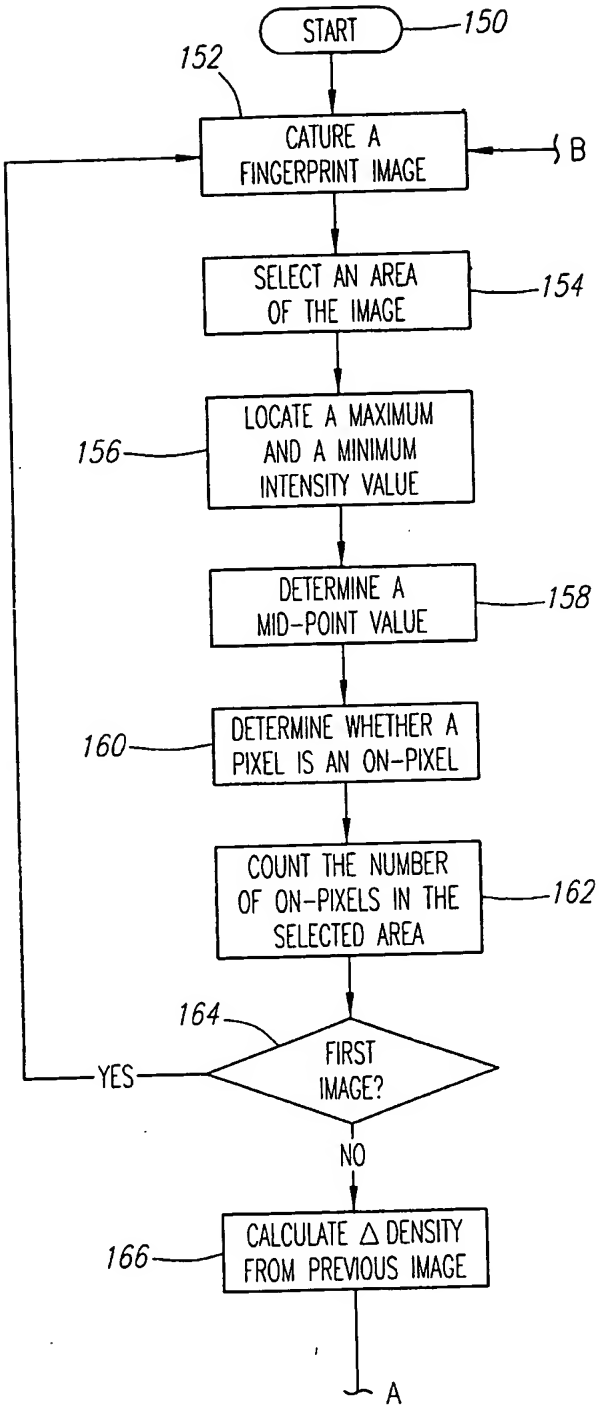


FIG. 3A

FIG. 3A
FIG. 3B

FIG. 3

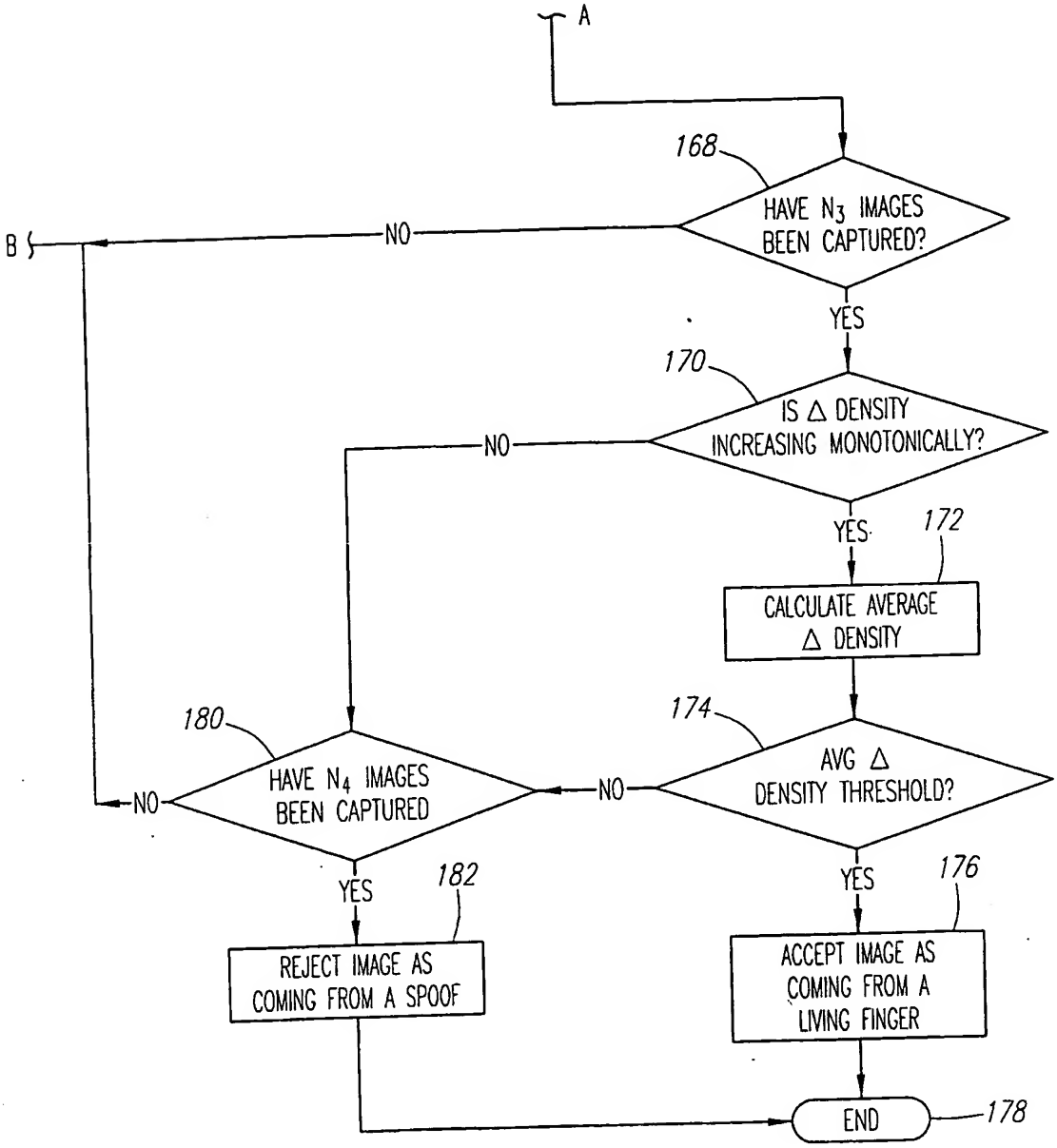

A
168
HAVE N_3 IMAGES BEEN CAPTURED?
NO
B
YES
170
IS Δ DENSITY INCREASING MONOTONICALLY?
NO
YES
172
CALCULATE AVERAGE Δ DENSITY
174
AVG Δ DENSITY THRESHOLD?
NO
YES
176
ACCEPT IMAGE AS COMING FROM A LIVING FINGER
180
HAVE N_4 IMAGES BEEN CAPTURED
NO
YES
182
REJECT IMAGE AS COMING FROM A SPOOF
END
178

FIG. 3B

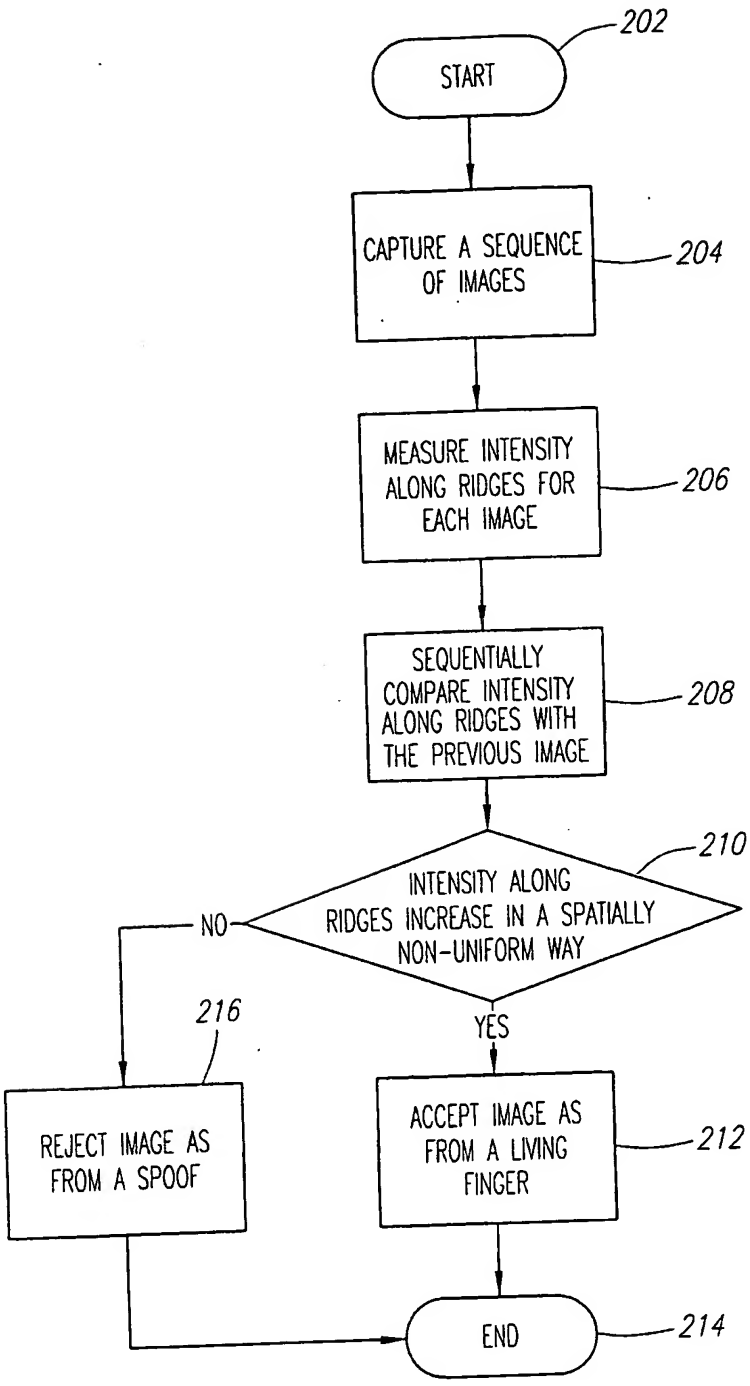

202
START
CAPTURE A SEQUENCE OF IMAGES
204
MEASURE INTENSITY ALONG RIDGES FOR EACH IMAGE
206
SEQUENTIALLY COMPARE INTENSITY ALONG RIDGES WITH THE PREVIOUS IMAGE
208
210
INTENSITY ALONG RIDGES INCREASE IN A SPATIALLY NON-UNIFORM WAY
NO
YES
216
REJECT IMAGE AS FROM A SPOOF
ACCEPT IMAGE AS FROM A LIVING FINGER
212
END
214

FIG. 4

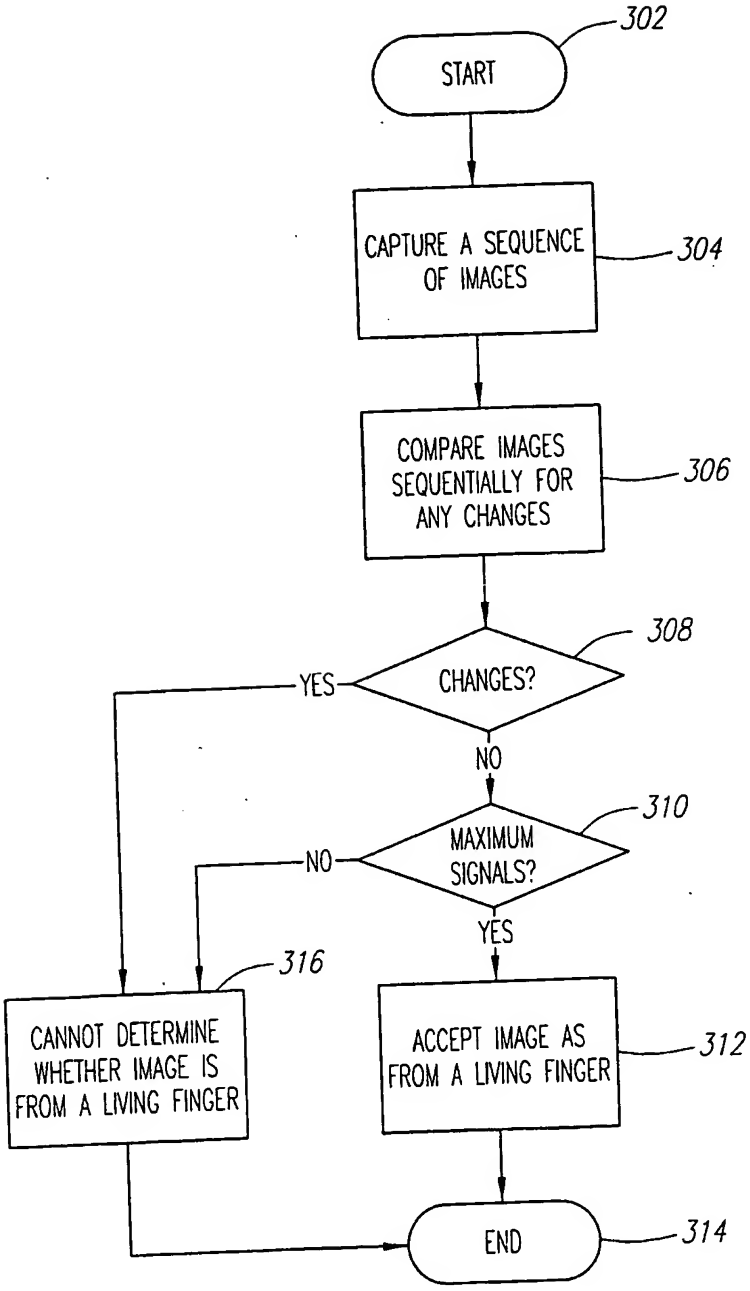

302
START
CAPTURE A SEQUENCE OF IMAGES
304
COMPARE IMAGES SEQUENTIALLY FOR ANY CHANGES
306
308
CHANGES?
YES
NO
310
MAXIMUM SIGNALS?
NO
YES
316
CANNOT DETERMINE WHETHER IMAGE IS FROM A LIVING FINGER
ACCEPT IMAGE AS FROM A LIVING FINGER
312
END
314

FIG. 5

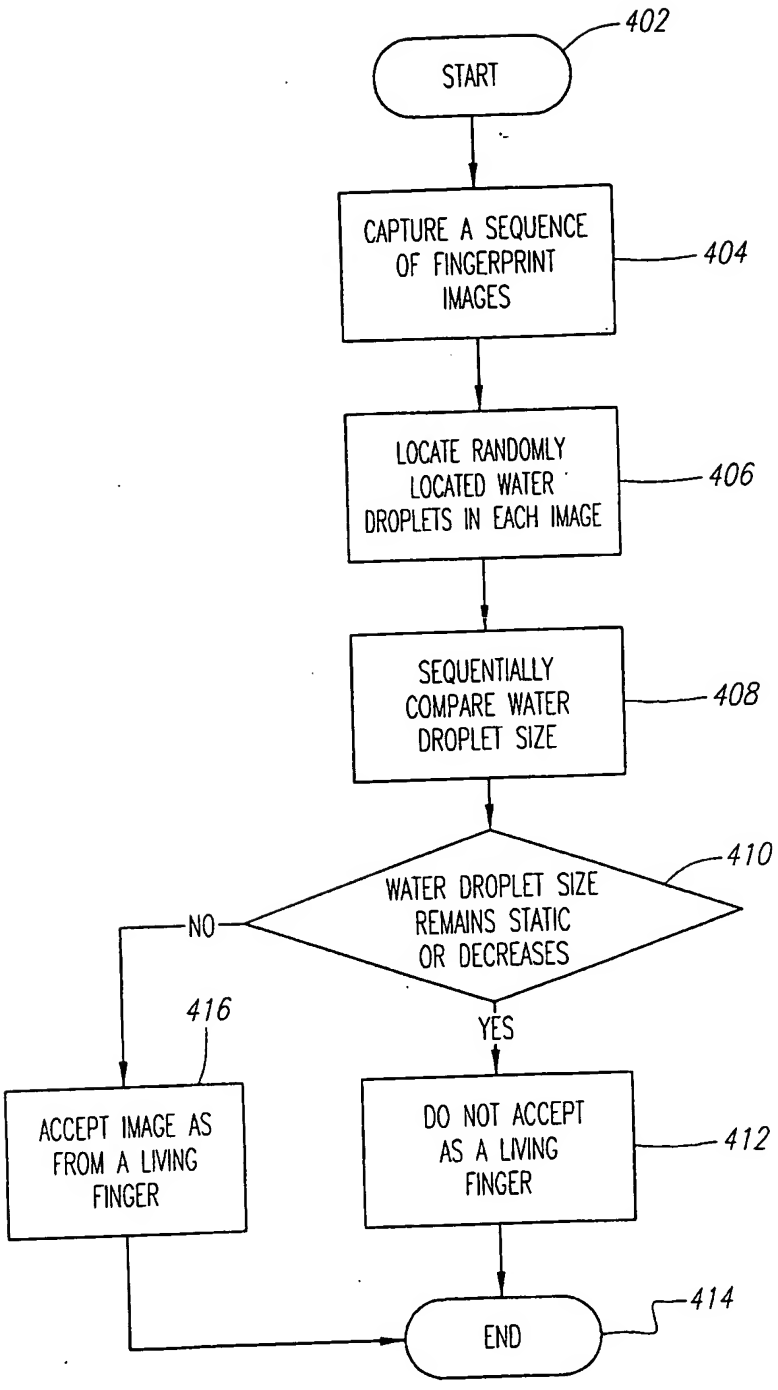

402
START
CAPTURE A SEQUENCE OF FINGERPRINT IMAGES
404
LOCATE RANDOMLY LOCATED WATER DROPLETS IN EACH IMAGE
406
SEQUENTIALLY COMPARE WATER DROPLET SIZE
408
WATER DROPLET SIZE REMAINS STATIC OR DECREASES
410
NO
YES
416
ACCEPT IMAGE AS FROM A LIVING FINGER
DO NOT ACCEPT AS A LIVING FINGER
412
END
414

FIG. 6

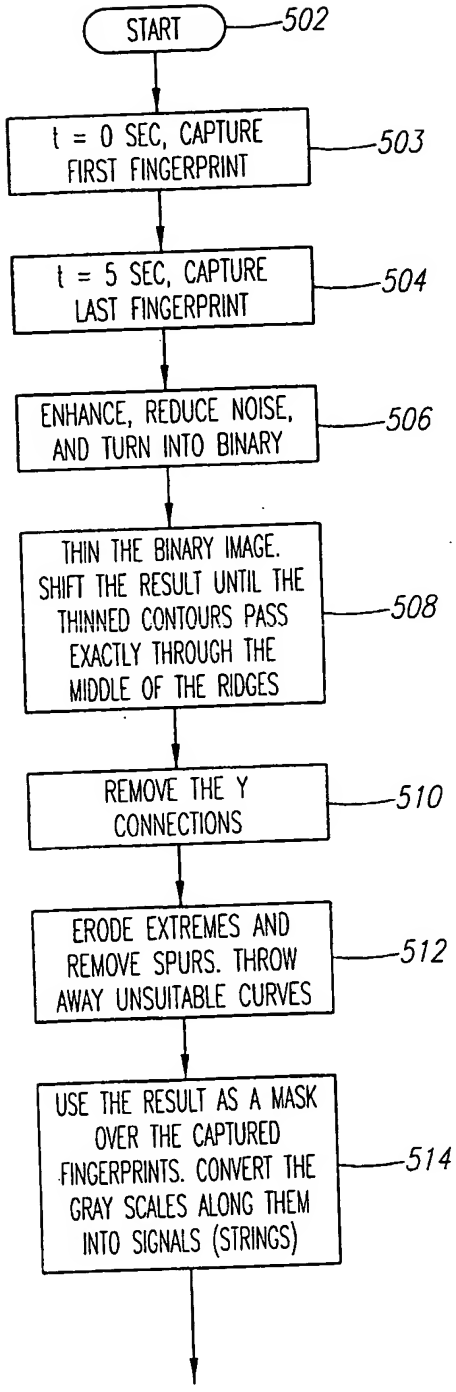

START
502
t = 0 SEC, CAPTURE FIRST FINGERPRINT
503
t = 5 SEC, CAPTURE LAST FINGERPRINT
504
ENHANCE, REDUCE NOISE, AND TURN INTO BINARY
506
THIN THE BINARY IMAGE. SHIFT THE RESULT UNTIL THE THINNED CONTOURS PASS EXACTLY THROUGH THE MIDDLE OF THE RIDGES
508
REMOVE THE Y CONNECTIONS
510
ERODE EXTREMES AND REMOVE SPURS. THROW AWAY UNSUITABLE CURVES
512
USE THE RESULT AS A MASK OVER THE CAPTURED FINGERPRINTS. CONVERT THE GRAY SCALES ALONG THEM INTO SIGNALS (STRINGS)
514

FIG. 7A

FIG. 7

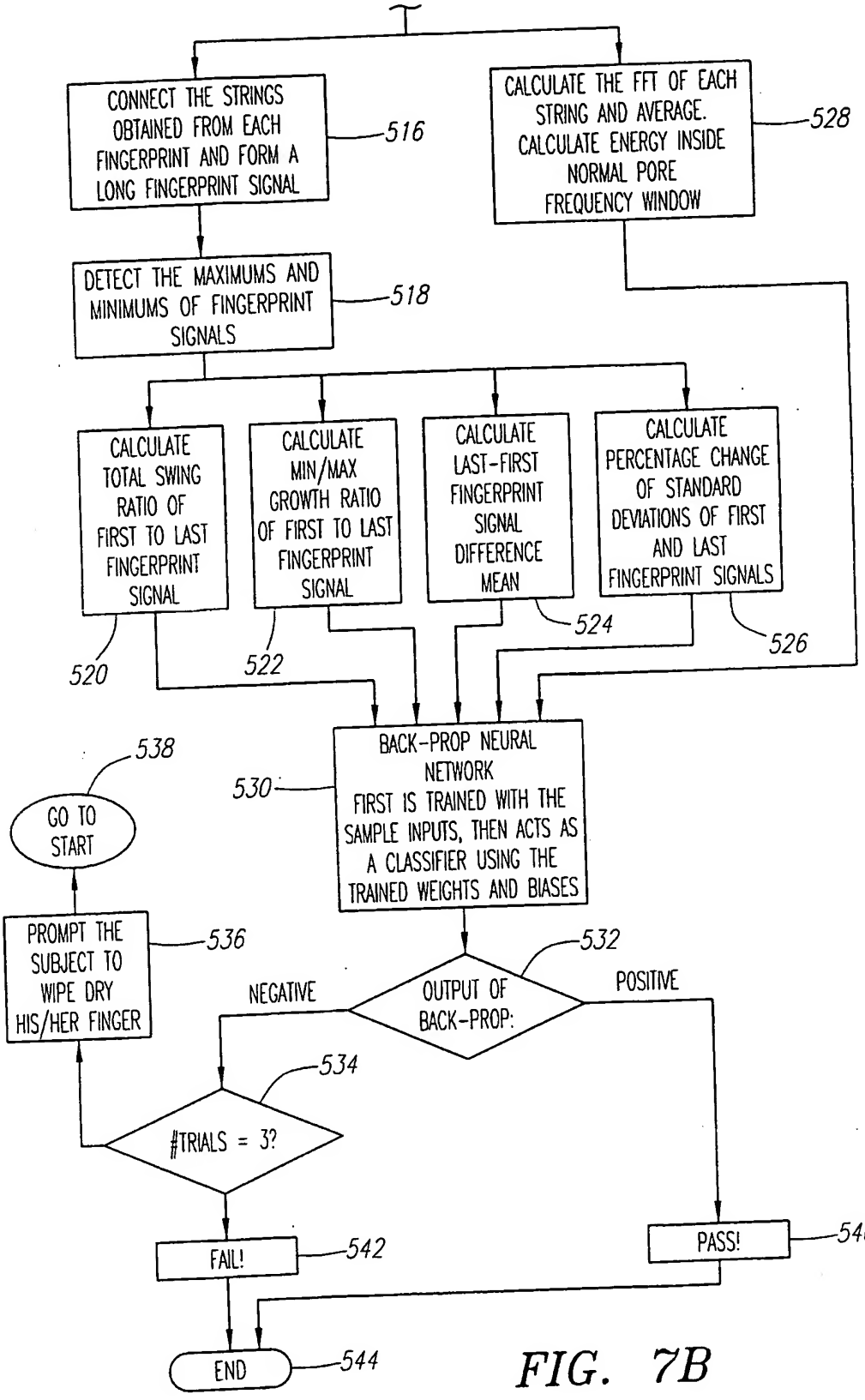

CONNECT THE STRINGS OBTAINED FROM EACH FINGERPRINT AND FORM A LONG FINGERPRINT SIGNAL
516
CALCULATE THE FFT OF EACH STRING AND AVERAGE. CALCULATE ENERGY INSIDE NORMAL PORE FREQUENCY WINDOW
528
DETECT THE MAXIMUMS AND MINIMUMS OF FINGERPRINT SIGNALS
518
CALCULATE TOTAL SWING RATIO OF FIRST TO LAST FINGERPRINT SIGNAL
CALCULATE MIN/MAX GROWTH RATIO OF FIRST TO LAST FINGERPRINT SIGNAL
CALCULATE LAST-FIRST FINGERPRINT SIGNAL DIFFERENCE MEAN
CALCULATE PERCENTAGE CHANGE OF STANDARD DEVIATIONS OF FIRST AND LAST FINGERPRINT SIGNALS
520
522
524
526
BACK-PROP NEURAL NETWORK FIRST IS TRAINED WITH THE SAMPLE INPUTS, THEN ACTS AS A CLASSIFIER USING THE TRAINED WEIGHTS AND BIASES
530
538
GO TO START
PROMPT THE SUBJECT TO WIPE DRY HIS/HER FINGER
536
OUTPUT OF BACK-PROP:
532
NEGATIVE
POSITIVE
#TRIALS = 3?
534
FAIL!
542
PASS!
540
END
544

FIG. 7B

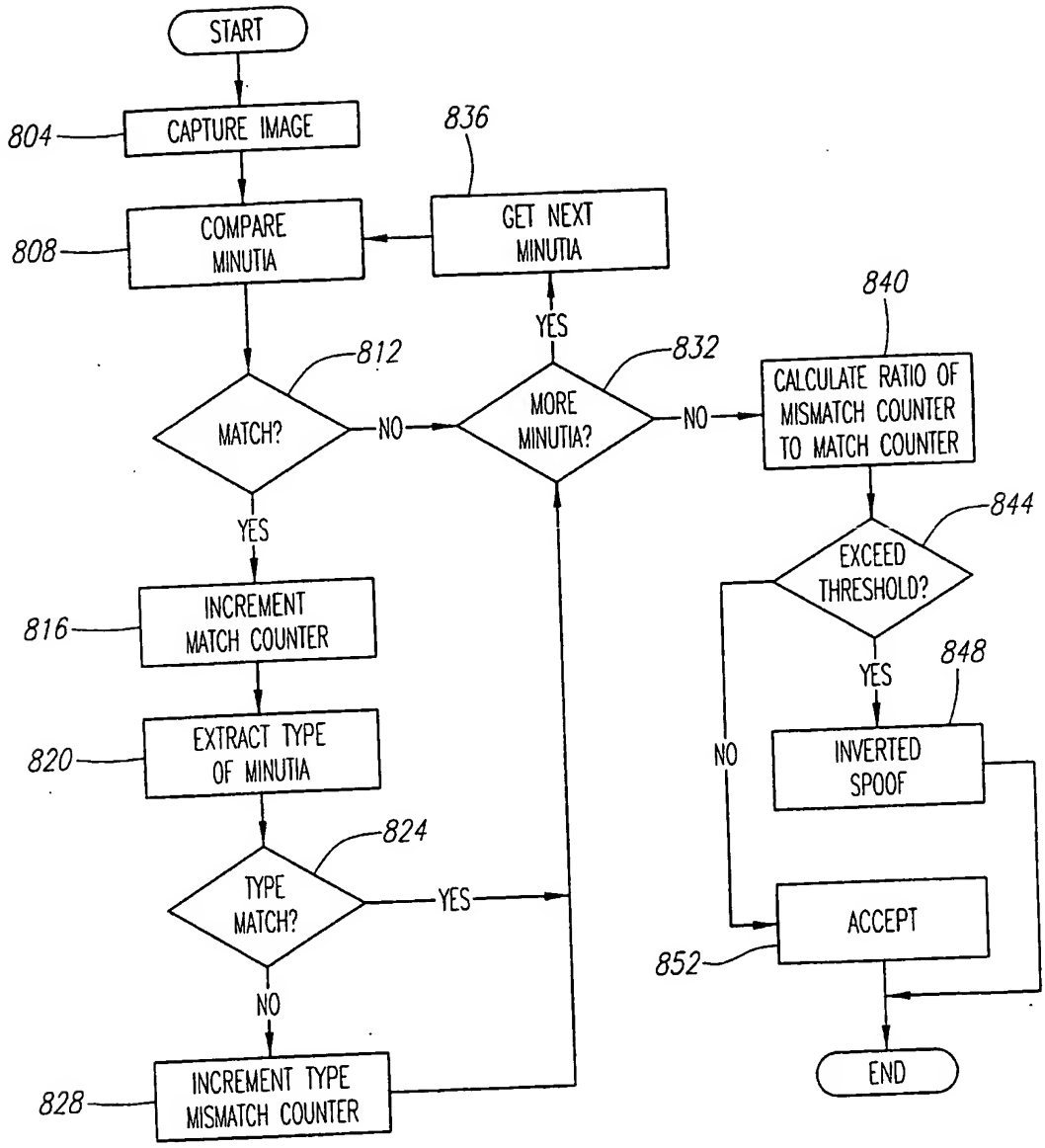

START
804
CAPTURE IMAGE
808
COMPARE MINUTIA
812
MATCH?
NO
YES
816
INCREMENT MATCH COUNTER
820
EXTRACT TYPE OF MINUTIA
824
TYPE MATCH?
YES
NO
828
INCREMENT TYPE MISMATCH COUNTER
836
GET NEXT MINUTIA
YES
832
MORE MINUTIA?
NO
840
CALCULATE RATIO OF MISMATCH COUNTER TO MATCH COUNTER
844
EXCEED THRESHOLD?
YES
NO
848
INVERTED SPOOF
852
ACCEPT
END

FIG. 8

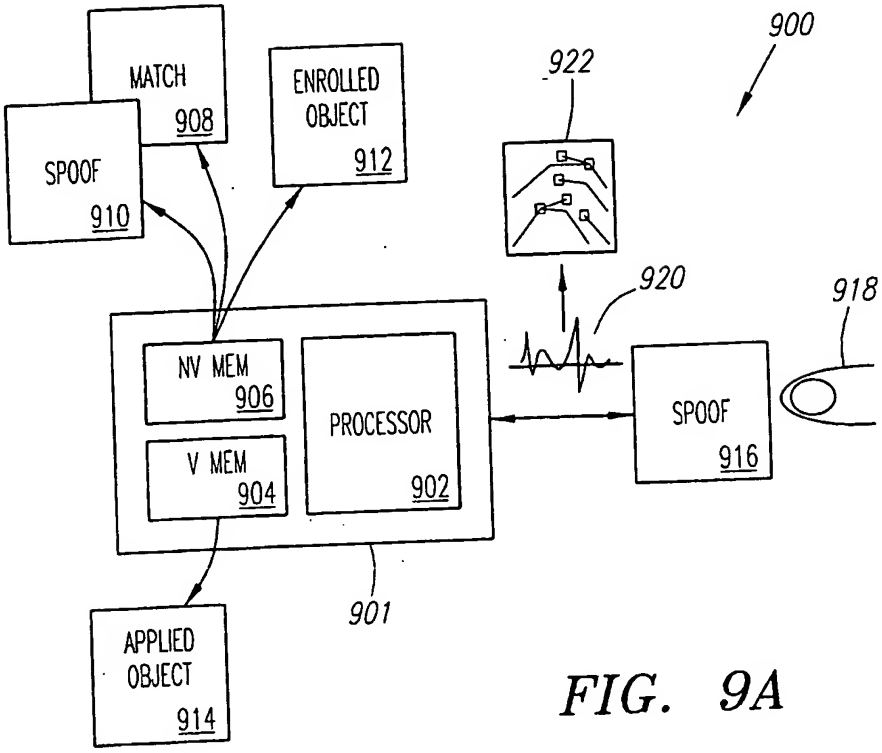

MATCH
908
ENROLLED OBJECT
912
SPOOF
910
900
922
920
918
NV MEM
906
PROCESSOR
902
V MEM
904
SPOOF
916
901
APPLIED OBJECT
914

FIG. 9A

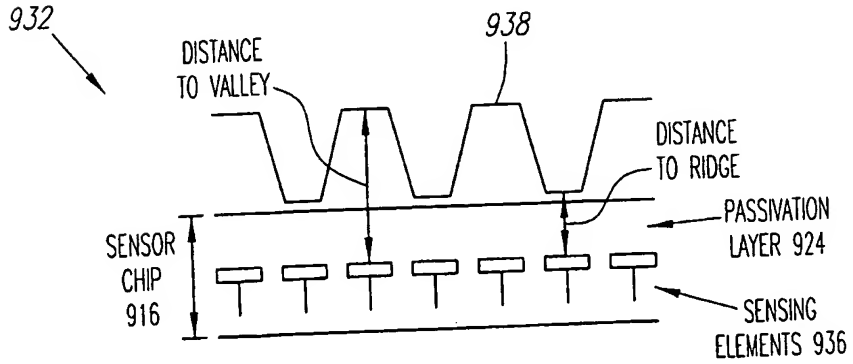

932
938
DISTANCE TO VALLEY
DISTANCE TO RIDGE
PASSIVATION LAYER 924
SENSOR CHIP 916
SENSING ELEMENTS 936

FIG. 9B

INTERNATIONAL SEARCH REPORT

Int[illegible]lication No
PCT/US 00/27782

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 A61B5/117 G07C9/00 G06K9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G07C A61B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 372 748 A (FUJITSU LTD) 13 June 1990 (1990-06-13) abstract ---	1,19,38
X	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 02, 26 February 1999 (1999-02-26) & JP 10 290796 A (NEC CORP), 4 November 1998 (1998-11-04) abstract ---	1,19,38
X	PATENT ABSTRACTS OF JAPAN vol. 015, no. 205 (P-1206), 27 May 1991 (1991-05-27) & JP 03 053385 A (NIPPON DENKI SEKIYURITEI SYST KK), 7 March 1991 (1991-03-07) abstract -----	1,17,19, 35,37,38

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February 2001	27/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Sonius, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int[redacted]lication No
PCT/US 00/27782

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0372748 A	13-06-1990	JP 2259969 A	22-10-1990
		JP 2695231 B	24-12-1997
		JP 2307176 A	20-12-1990
		JP 2774313 B	09-07-1998
		JP 2708051 B	04-02-1998
		JP 3087981 A	12-04-1991
		JP 2144685 A	04-06-1990
		CA 2003131 A,C	25-05-1990
		DE 68918244 D	20-10-1994
		DE 68918244 T	02-02-1995
		KR 9302346 B	29-03-1993
		US 5088817 A	18-02-1992
JP 10290796 A	04-11-1998	JP 2962274 B	12-10-1999
JP 03053385 A	07-03-1991	NONE	

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

Viering, Jentschura & Partner
Steinsdorfstr. 6
80538 München
ALLEMAGNE

VIERING, JENTSCHURA & PARTNER
Erhalten / Received
- 7. Dez. 2001
Frist / Due Date: 07. Dez. 2001

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Rule 71.1)

	Date of mailing *(day/month/year)* 05.12.2001
Applicant's or agent's file reference P 21723	IMPORTANT NOTIFICATION

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US00/27782	06/10/2000	07/10/1999

Applicant
VERIDICOM, INC. et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Ullrich, C Tel.+49 89 2399-2322

Form PCT/IPEA/416 (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
249/118-PCT		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US 00/ 27782	06/10/2000	07/10/1999
Applicant		
VERIDICOM, INC.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequenuy to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 9a

   [X] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

12

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
P 21723		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US00/27782	06/10/2000	07/10/1999
International Patent Classification (IPC) or national classification and IPC		
A61B5/117		
Applicant		
VERIDICOM, INC. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 11 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
07/05/2001	05.12.2001
Name and mailing address of the international preliminary examining authority:	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Rick, K Telephone No. +49 89 2399 7246

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US00/27782

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:
Description, pages:

1,2,4-10,12-15, 17-36	as originally filed			
3a-3b,11,16	as received on	14/11/2001	with letter of	13/11/2001

Claims, No.:

1-28	as received on	14/11/2001	with letter of	13/11/2001

Drawings, sheets:

1/11-10/11	as originally filed			
11/11	as received on	14/11/2001	with letter of	13/11/2001

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

☐ the description, pages:
☒ the claims, Nos.: 29-38
☐ the drawings, sheets:

5. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)
see separate sheet

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-28
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-28
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-28
	No:	Claims	

2. Citations and explanations
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Re Item I

Basis of the report

1. The amendments filed with the letter dated 13.11.2001 introduce subject-matter which extends beyond the content of the application as filed, contrary to Article 34(2)(b) PCT. The amendments concerned are the following (all references are related to the amended set of claims):

Claims 9, 10 and 12:

- The applicant has deleted the following feature "between the fingerprint signal of the initial image and the fingerprint signal of the subsequently captured image" and added "between the plurality of electrical representations" (p. 38, l. 33; p. 39, l. 3 and 11). A free choice of images respectively electrical representations to be compared is not supported by the originally filed application. Hence the deletion resp. addition of these features does not satisfy the criterion set forth in Article 34(2)(b) PCT.

2. The examination has been carried out as if the above mentioned subject-matter, which goes beyond the original disclosure, had not been introduced.

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Reference is made to the following documents:

D1: PATENT ABSTRACTS OF JAPAN vol. 015, no. 205 (P-1206), 27 May 1991 (1991-05-27) & JP 03 053385 A (NIPPON DENKI SEKIYURITEI SYST KK), 7 March 1991 (1991-03-07)

D2: EP-A-0 372 748 (FUJITSU LTD) 13 June 1990 (1990-06-13)

D3: PATENT ABSTRACTS OF JAPAN vol. 1999, no. 02, 26 February 1999 (1999-02-26) & JP 10 290796 A (NEC CORP), 4 November 1998 (1998-11-04)

2. Document D1 is regarded as closest prior art with respect to the subject-matter of claim 1. D1 discloses (the references in parentheses applying to this document):
A biometric sensing system comprising
- an image capture device (fingerprint set checking part 102, D1, abstract) configured to capture images of an applied finger over a predetermined period of time and create a plurality of electrical representations of the applied finger using the captured images;
- a spoof detection module (forgery input discriminating part 103, D1, abstract) configured to compare the variable density value of image elements of the electrical representations with a stored variable density value indicative of a non-living applied finger.

The subject-matter of claim 1, amended as requested in section VIII, differs from this known device in that the spoof detection module is configured to analyse the plurality of electrical representations for relative temporal anomalies of the density or intensity, as measured between the plurality of electrical representations.

Such an arrangement provides for the advantage that there is a direct comparison of the density or intensity pattern as extracted from subsequently captured images and therefore no stored reference values are needed in order to identify a non-living applied finger and reject it as a spoof.

The biometric sensing system according to D2 comprises an image capture device (personal identification unit 43, D2, col 10, l. 49-56); a minutia matching module (D2, col 10, l. 56 to col.11, l. 24) and a spoof detection module (biological object detection unit 6, D2, col. 6, l. 38) comparing the spectrally resolved optical signals of an applied finger in a "pressed" and a "not pressed" state (D2, col. 6, l. 48 to col. 7, l. 22) to identify a non-living applied finger.

In the biometric sensing system according to D3 again a physical stimulus (warming, cooling) is applied to a finger and the change of a biological signal in response to said stimulus is measured to identify a non-living applied finger (D3, abstract).

The subject-matter of claim 1 differs from the known devices of D2 and D3 in that

the spoof detection module is merely software implemented and thus no additional hardware is needed to add the spoof detection module to an existing personal identification system. Furthermore no change of the physical condition of the finger (pressed - not pressed, cold - warm) is needed to identify a non-living applied finger and reject it as a spoof.

Claim 1 thus meets the requirements of Article 33(2)-(4) PCT as there is no obvious suggestion of this configuration in the available prior art.

3. Since claim 14 merely describes the according method to apparatus claim 1, it meets the requirements of Article 33(2)-(4) PCT either.

4. Claims 2-13 and 15-28 dependent thereon and amended as requested in section VIII define further advantageous embodiments and as such also meet the requirements of Article 33 PCT.

Re Item VIII
Certain observations on the international application

1. Claim 1 does not meet the requirements of Article 6 PCT in that the matter for which protection is sought is not clearly defined. Since it is clear from the description (p. 9, l. 31 to p. 10, l. 2 and p. 11, l. 24-32), that the images are captured and subsequently used to create the plurality of electrical representations, a clear link is missing in claim 1 between the capturing of said images and the creation of said electrical representations, as it can be found e.g. in the according method of amended independent claim 14.

2. The term of amended claim 6 to "accept the applied finger as a living finger when the pixel intensity does not increase" is in contradiction to the description rejecting the applied finger as a spoof under the same condition (p. 6, l. 11-14 and p. 21, l. 13-18), thereby rendering the definition of the subject-matter of said claim unclear (Article 6 PCT).

The same objection has to be raised for amended claim 18 ("is less than a threshold") in comparison to the description on p. 16, l. 13 to p. 17, l. 5 and amended claim 24 ("rejecting the fingerprint signal when the signal difference mean is indicative of a living finger") in comparison to the description on p. 30, l. 22 to p. 31, l. 4.

3. Furthermore, the inconsistent use of the terms "electrical representation" and "image" in amended claims 17 and 20 for obviously the same subject-matter leaves the reader in doubt as to the meaning of the technical features to which they refer, thereby rendering the definition of the subject-matter of said claims unclear (Article 6 PCT).

The skin resistance and temperature safeguards, however, can easily be circumvented by warming up an artificial or dead finger or by designing an artificial finger with a resistance similar to a true finger.

Still other fingerprint authentication systems utilize other medical measurements to determine whether the fingerprint presented is from a living finger or a spoof. One such system is described in U.S Patent No. 5,719,950, entitled: "Biometric, Personal Authentication System" of Osten et al., issued February 17, 1998, which incorporates biological measurements, such as electrocardiograph signals and blood pressure, in conjunction with a fingerprint scan to determine whether the fingerprint presented originates from a living finger. Disadvantages of these systems include their complexity, large size and high cost. In addition, systems which probe medical signals of a person are highly intrusive.

There is a need, therefore, for an improved method for distinguishing a living finger from a spoof. In particular, the method should accurately discern between the two without being overly intrusive. The method also should not significantly increase the size or cost of the system.

Reference is made to a few patent documents. The first is JP3053385, a Japanese patent abstract by Morita Koichiro, for applicant Nippon Denki Sekituritei Syst KK, entitled "Feature Extraction Device". This abstract discloses a sensor for detecting positional coordinates of minutiae. First, a fingerprint set checking part 102 detects the change of variable density of picture elements in a prescribed position, based on a series of pictures repeatedly taken by an industrial television. Part 102 confirms that the placement of a fingerprint over the industrial television is completed. Next, a forgery input discriminating part 103 compares the variable density of the picture elements in the prescribed position with stored, static, threshold values. If the stored, static, threshold values differ from the variable density value, then the fingerprint is considered a forged finger. If not, then an input picking control part selects the picture, and then stores it in a picture storage part 105.

Another document is JP10290796, another Japanese patent abstract, this one by Fukuzumi Shinichi, for applicant NEC Corp., entitled "Method and Device for Identifying Living Body". Here a device is shown that applies a warming or cooling stimulation to a finger. The duration, strength, and presentation levels of the warming or cooling stimulus are monitored

and controlled by the device. Based on the response to the warming or cooling stimulus, the finger is identified as a living body or a replica.

Still another document is EP0372748, a European patent application, by Seigo Igaki et al, for applicant Fujitsu Limited, entitled, "Fingerprint-Detecting Device". This reference discloses an optical fingerprint sensor. Like JP10290796, EP0372748 discloses a system whereby a physical stimulus, in this instance pressure, is applied to a finger. The light source for the optical sensor, and a light detector are used to determine the spectral reflectance of the received light, and thereby identify a real, versus a forged, finger, by noting that the spectral reflectance of a finger under pressure is less than the spectral reflectance of a finger without pressure.

SUMMARY OF THE INVENTION

A method and apparatus for employing spoof detection for a biometric sensing device is provided, the features of which are set forth in the independent claims below. The invention employs a number of computer implemented techniques designed to distinguish between a living and a non-living biometric, particularly a fingerprint. Anomalies of an electrical representation of a fingerprint, captured from the biometric sensing device, are analyzed using any number of steps designed to detect certain characteristics that are difficult to spoof and largely unique to a living finger.

According to one embodiment, a solid state fingerprint sensor is employed. One such solid state sensor is a capacitive sensor that captures fingerprints by electrical means. Depth is determined by electric field strength, which is inversely proportional to distance. Because capacitive fingerprint sensors require a three-dimensional object, they do not accept a photographic copy of a true fingerprint. In addition, in order for these sensors to capture a fingerprint, the finger or object presented to the sensor must have electrostatic characteristics similar to the skin on a living finger. This will eliminate fingerprints from plastic or rubber molded fingers, as these materials are non-conductive.

The method further relies on additional characteristics of living fingers that cannot be easily replicated by an artificial, dead or severed finger. For example, living skin has the

location but can be distributed and "logically" arranged as depicted in FIG. 9A. The figure and description is intended to capture this logical arrangement.)

While the program code is ultimately embodied in a system as depicted, for instance, in FIG. 9A, the program code can be sequences of instructions for causing a processor (or distributed processors) to perform the functionalities described above (and more particularly below). The program code, or "software product", can be stored in a tangible medium, such as a CD-ROM, floppy disk, or a computer memory, for instance a shared memory or shared disk on a networked computer system. Further still, the software product can be embodied in downloadable, and perhaps compressed and encrypted, computer data files that are later loaded and executed (or interpreted) by a general purpose computer or an image capture device. According to one embodiment, the invention is completely represented by the spoof detection module software alone -- and can be sold as a stand-alone product augmenting or improving an existing image capture device and/or biometric matching module.

The sensor 916 is preferably a capacitive fingerprint sensor. It is further described with reference to FIG. 9B, to which we now turn.

FIG. 9B shows a diagram of a fingerprint imaging device 932. In normal operation, the fingerprint imaging device 932 used techniques derived from Columbus law to determine the location of ridges and valleys in a fingerprint surface 938. By modeling each sensing element 936 in the sensor chip 916 as one plate in a capacitor, the finger surface 938 (that is, the ridges and valleys) being the second plate in the capacitor, it is possible to measure a relative distance between the ridges and valleys to construct an electrical representation of the fingerprint. According to one embodiment, a passivation layer 924 is disposed over the sensing elements 936 to form the capacitor at the ridges.

Turning back to FIG. 9A, when the sensor 916 detects an applied object 918 and captures an image, the individual sensing elements 936 create an electrical representation 920 of the surface 938 of the skin. In an abstract form, the electrical representation may be modeled as the fingerprint 922, wherein particular minutiae are highlighted by boxes only for the purpose of illustration. What is captured, however, is more than simply data representative of ridges and valleys in a fingerprint; anomalies, or "noise" (as is mentioned above) in the image will inevitably occur. These anomalies are discarded by prior systems, but here they are used to computationally analyze the electrical representation 920 for indicia of a living finger.

The system then determines whether the average intensity is increasing monotonically for the sequence of captured images (step 120). Monotonically increasing average intensity indicates that the applied object is warming up which is an indication of a living finger. A monotonically increasing average intensity is characterized by, for instance, 80% of the captured images having a positive delta average intensity.

For example, if six images are captured, the same as in the above example, then the five delta average intensities are +10, +10, +10, +10 and +10. Since 100% of the images exhibit an increase in average intensity, the average intensity increases monotonically.

If the average intensity increases monotonically (step 120), then the system determines whether the average delta intensity is greater than a predetermined threshold amount (step 122). In on embodiment, the predetermined threshold is 10%. This value is selected based on experimentation. If the average delta intensity is greater than the predetermined threshold amount (step 122), then the image is accepted as coming from a living finger (step 124) and the process ends in step 126. All counters are reset at step 126. It is noted that steps 120 and 122 may be reversed in sequence or executed in parallel.

After N1 image have been captured, if the average intensity does not increase monotonically (step 120), or the average delta average intensity does not exceed the predetermined threshold amount (step 122), then a decision cannot be made as to whether the captured image is coming from a living finger or a spoof. When the decision cannot be made in the minimum time, e.g. 1.2 seconds for 6 images captured at a rate of 0.2 seconds, it is determined whether N2 images have been captured (step 128). N2 is the maximum number of images captured for the system to make a decision. If N2 images have not been captured (step 128), then an additional image is captured (step 104) and after the time delay (step 109) until N2 images have been captured or until the system determines that the image is coming from a living finger. In one embodiment, the value of N2 is 15 (or the capture time is 3 seconds).

The average intensity of the additional image is calculated in step 106. The delta average intensity is calculated (step 110). The average delta average intensity is calculated (step 118). The system then determines whether the average intensity increases monotonically (step 120) and whether the average delta average intensity is greater than the threshold amount (step 122) as described above. If the average intensity increases

CLAIMS

What is claimed is:

1. A biometric sensing system (900) comprising:

an image capture device (916) configured to capture images (922) of an applied finger (918) over a predetermined period of time and create a plurality of electrical representations (920) of the applied finger (918);

a spoof detection module (910) configured to analyze the plurality of electrical representations (920) for relative temporal anomalies of intensity, or relative temporal anomalies of density, as measured between the plurality of electrical representations (920), indicative of a living applied finger (918); and

a minutia matching module (908) for matching minutia from one or more of the plurality of electrical representations (920) of the applied finger (918) with minutia of an enrolled finger (912).

2. The biometric sensing system (900) of claim 1, wherein the spoof detection module (910) is configured to employ an average intensity technique to detect and classify the anomalies, the average intensity technique configured to cause the system (900) to calculate an average intensity for each of the plurality of electrical representations (920).

3. The biometric sensing system (900) of claim 2, wherein the average intensity technique is further configured to cause the system (900) to accept the applied finger (918) as a living finger when the average intensity increases monotonically over the plurality of electrical representations (920).

4. The biometric sensing system (900) of any of the above claims, wherein the spoof detection module (910) is configured to employ a pixel density technique to detect and classify the anomalies, the pixel density technique causing the system (900) to determine an ON-pixel value based upon a first electrical representation, determine pixel count for each electrical representation in the plurality of electrical representations (920), wherein the counted pixels exceed the ON-pixel value, and calculate a delta pixel count over the plurality of electrical representations (920).

5. The biometric sensing system (900) of claim 4, wherein the pixel density technique is further configured to cause the system (900) to accept the applied finger (918) as a living

finger when the delta pixel count increases monotonically over the plurality of electrical representations.

6. The biometric sensing system (900) of any of the above claims, wherein the spoof detection module (910) is configured to employ a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system (900) to measure pixel intensity along ridges in each of the plurality of electrical representations (920), determine whether the pixel intensity increases in a spatially non-uniform manner, and accept the applied finger (918) as a living finger when the pixel intensity does not increase in the specially non-uniform manner.

7. The biometric sensing system (900) of any of the above claims, wherein the spoof detection module (910) is configured to employ a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system (900) to measure pixel intensity values along contours of ridges in each of the plurality of electrical representations (920), binarize the pixel intensity values, measure the pixel intensity various along the ridges, and accept the applied finger as a living finger when the measured pixel intensity variations are roughly sinusoidal.

8. The biometric sensing system (900) of any of the above claims, wherein the spoof detection module (910) is configured to employ a water droplet differential technique to detect and classify the anomalies, the water droplet differential technique configured to cause the system (900) to locate a first water droplet positioned within an electrical representation in the plurality of electrical representations (920), locate a like-positioned water droplet within a subsequent electrical representation of the plurality of electrical representations (920), compare a size of the first water droplet with a size of the like-positioned water droplet, and accept the applied finger (918) as a living finger when the size of the like-positioned water droplet is larger than the size of the first water droplet.

9. The biometric sensing system (900) of any of the above claims, wherein the spoof detection module (910) is configured to employ a fingerprint vitality technique to detect and classify the anomalies, the fingerprint vitality technique configured to cause the system (900) to compare a total swing ratio between the plurality of electrical representations (920).

10. The biometric sensing system (900) of claim 9, wherein the fingerprint vitality technique is further configured to cause the system (900) to compare a minimum or a maximum growth ratio between the plurality of electrical representations (920).

11. The biometric sensing system (900) of claim 9 or 10, wherein the fingerprint vitality technique is further configured to cause the system (900) to compare last to first fingerprint signal difference mean between the plurality of electrical representations (920).

12. The biometric sensing system (900) of claim 9, 10 or 11, wherein the fingerprint vitality technique is further configured to cause the system (900) to compare a percentage change of standard deviation between the plurality of electrical representations (920).

13. The biometric sensing system (900) of claim 9, 10, 11 or 12, further comprising a neural network, wherein the neural network is configured to perform the step of comparing.

14. A computer implemented method for detecting a spoof of a living finger, comprising:

capturing images (922) of an applied finger (918) over a predetermined period of time;

creating a plurality of electrical representations (920) of the applied finger (918) using the captured images (922);

analyzing relative temporal anomalies of intensity or relative temporal anomalies of density for each of the plurality of electrical representations (920); and

matching minutia from one or more of the plurality of electrical representations (920) of the applied finger (918) with minutia from an enrolled finger (912), when the step of analyzing indicates that the applied finger (918) is a living finger.

15. The method of claim 14, wherein the step of analyzing comprises:

calculating an average intensity for each of the plurality of electrical representations (920) accepting the applied finger (918) as a living finger when the average intensity, as sequentially measured over the plurality of electrical representations (920) increases monotonically.

16. The method of claim 15, further comprising:

calculating an average change in the average intensity of the plurality of electrical representations (920); and

AMENDED SHEET

accepting the applied finger (918) as a living finger when the average change in the average intensity is greater a threshold average change in the average intensity value.

17. The method of claim 14, 15 or 16, wherein the step of analyzing comprises:

selecting a portion of a first image in the plurality of electrical representations (920)

determining an ON-pixel value based upon intensity values in the portion of the first image;

counting a number of pixels exceeding the ON-pixel value in the portion of the first image;

repeating the above steps of selecting, determining, and counting for a next image in the plurality of electrical representation;

calculating an average density value between the first image and the next image; and

accepting the applied finger (918) as a living finger when the average density value increases monotonically.

18. The method of claim 17, further comprising:

calculating an average change in average density between the plurality of electrical representations (920); and accepting the applied finger (918) as a living finger when the average change in average density is less than a threshold average change in average density value.

19. The method of claim 14, 15, 16, 17, or 18, wherein the step of analyzing comprises:

measuring intensity along ridges in each of the plurality of electrical representations (920);

comparing the intensity along the ridges from each electrical representation with the intensity along the ridges from a coterminously captured image (922);

determining whether the intensity along the ridges increases in a spatially non-uniform manner; and

accepting the applied finger (918) as a living finger when the intensity along the ridges increases in a spatially non-uniform manner.

20. The method of claim 14, 15, 16, 17, 18 or 19, wherein the step of analyzing comprises:

locating water droplets in each of the plurality of electrical representations (920);

AMENDED SHEET

comparing a size of the water droplet in each of the plurality of electrical representations (920) with a size of the water droplet in a subsequently captured image (922) in the plurality of the electrical representations (920);

accepting the applied finger (918) as a living finger when the water droplet size increases over time, as represented in the plurality of electrical representations (920).

21. The method of claim 14, 15, 16, 17, 18, 19 or 20, wherein the step of analyzing comprises:

digitally processing a first electrical representation from the plurality of electrical representations (920);

saving the digitally processed electrical representation as a mask;

applying the mask over subsequent electrical representations;

converting the result of the mask of the subsequent electrical representations into fingerprint strings;

connecting the fingerprint strings into a fingerprint signal for each image;

analyzing the fingerprint signal for anomalies; and

accepting the fingerprint signal when the anomalies are indicative of a living finger.

22. The method of claim 21,

wherein analyzing the fingerprint signal for anomalies comprises calculating a total swing ratio of a first fingerprint signal to a last fingerprint signal; and

accepting the fingerprint signal when the total swing ratio is indicative of a living finger.

23. The method of claim 21 or 22,

wherein analyzing the fingerprint signal for anomalies comprises:

calculating a minimum or maximum growth ratio as measured between a first fingerprint signal and a last fingerprint signal; and

accepting the fingerprint signal when the growth ratio is indicative of a living finger.

24. The method of claim 21, 22 or 23,

wherein analyzing the fingerprint signal for anomalies comprises:

calculating a first fingerprint signal to a last fingerprint signal difference mean; and

rejecting the fingerprint signal when the signal difference mean is indicative of a living finger.

25. The method of claim 21, 22, 23 or 24;

wherein analyzing the fingerprint signal for anomalies comprises calculating a percentage change of standard deviation between a first fingerprint signal and a last fingerprint signal; and

accepting the fingerprint signal when the signal difference mean is indicative of a living finger.

26. The method of claims 21, 22, 23, 24 or 25, further comprising:

calculating a spatial frequency of peaks in the fingerprint strings;

calculating a total energy for the fingerprint strings, based on the spatial frequency; and

accepting the fingerprint signal as a living finger when the average energy is above a threshold total energy.

27. The method of claim 21, 22, 23, 24, 25 or 26 further comprising, prior to accepting the fingerprint signal as a living finger sending the anomalies to a neural network for classification.

28. A computer software product having stored therein sequences of instructions for causing one or more processors to perform the methods recited in above claims 14 through 27.

AMENDED SHEET

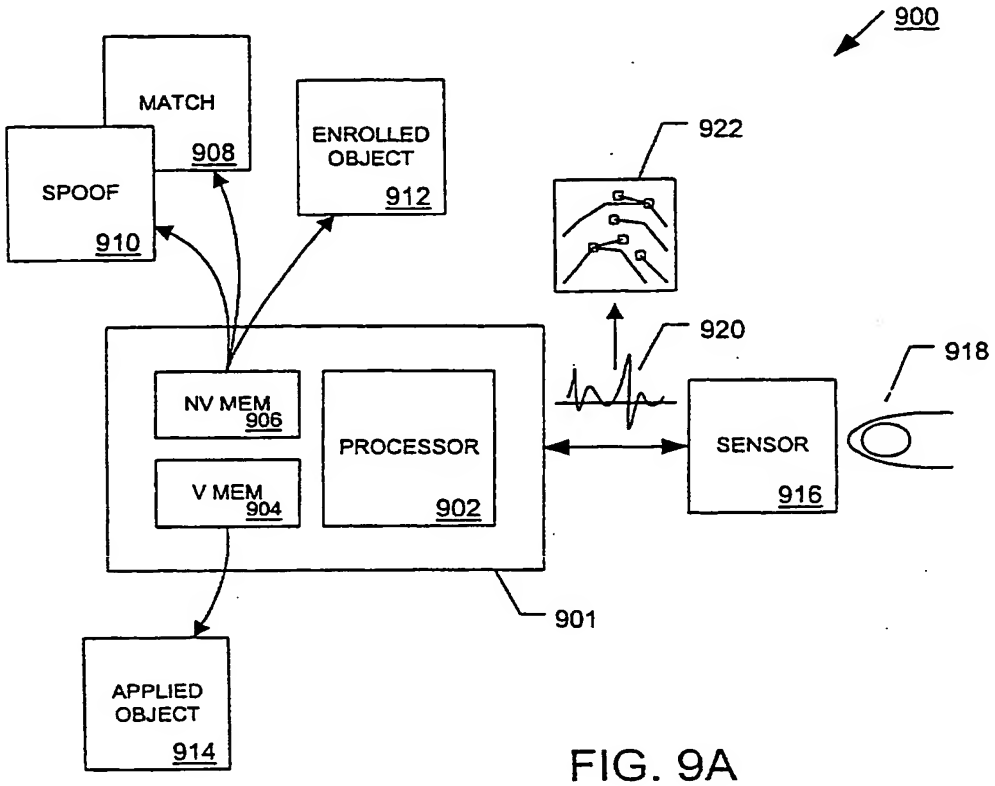

900
MATCH
908
SPOOF
910
ENROLLED OBJECT
912
922
920
918
NV MEM
906
V MEM
904
PROCESSOR
902
SENSOR
916
901
APPLIED OBJECT
914

FIG. 9A

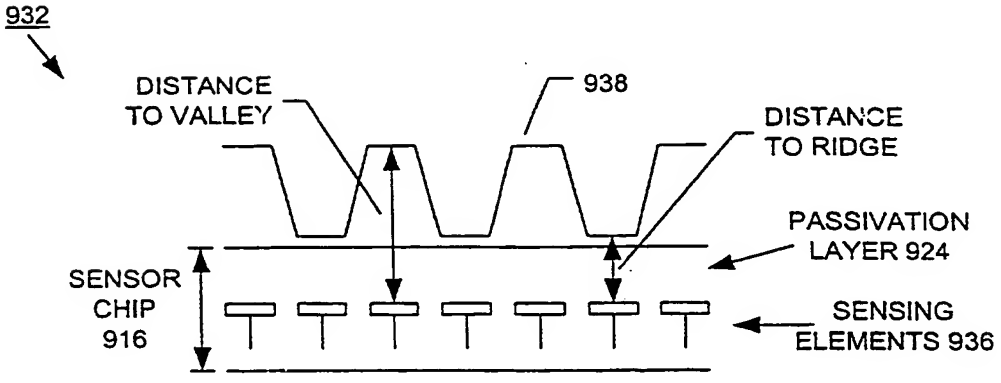

932
DISTANCE TO VALLEY
938
DISTANCE TO RIDGE
PASSIVATION LAYER 924
SENSOR CHIP 916
SENSING ELEMENTS 936

FIG. 9B

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2001 (01.11.2001)

PCT

(10) International Publication Number
WO 01/82218 A1

(51) International Patent Classification[7]: G06K 9/60, H03G 3/20

(21) International Application Number: PCT/US01/12921

(22) International Filing Date: 20 April 2001 (20.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/560,702 27 April 2000 (27.04.2000) US

(71) Applicant: VERIDICOM, INC. [US/US]; 2040 Martin Avenue, Santa Clara, CA 95050 (US).

(72) Inventors: YEH, Hsueh-Li; c/o Veridicom, 2040 Martin Avenue, Santa Clara, CA 95050 (US). CHENG, Ericson; c/o Veridicom, 2040 Martin Avenue, Santa Clara, CA 95050 (US). RUSSO, Anthony; c/o Veridicom, 2040 Martin Avenue, Santa Clara, CA 95050 (US).

(74) Agent: WOLFF, Jason, W.; Lyon & Lyon LLP, 47th Floor, 633 West Fifth Street, Los Angeles, CA 90071-2066 (US).

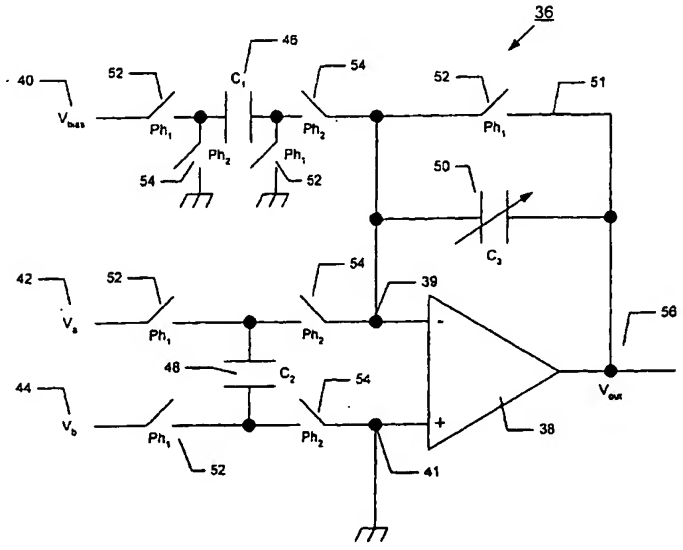
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: AUTOMATIC GAIN AMPLIFIER FOR BIOMETRIC SENSOR DEVICE



(57) Abstract: An automatic gain amplifier is disclosed that dynamically improves the quality of scanned biometric information. According to one embodiment, an image distribution of the scanned biometric is generated. Next, areas of higher image distribution are identified. An iterative process of adjusting the gain of, for instance, a capacitive sensing, is employed until an optimum separation of the areas of higher image distribution is achieved. Once the optimum separation is achieved, the gain is applied to the biometric sensing device so that biometric information can be scanned with improved image clarity. Electronic circuitry and software for implementing the methods are disclosed.

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE OF THE INVENTION

AUTOMATIC GAIN AMPLIFIER FOR BIOMETRIC SENSOR DEVICE

BACKGROUND

1. Field of the Invention.

The present invention is related to an automatic gain amplifier, and more particularly to an automatic gain amplifier used in a biometric sensing device.

2. Background Information.

In biometric imaging devices, for example optical-based or electrical properties-based fingerprint scanning devices, a user places a finger on a fingerprint sensor. The fingerprint sensor scans the fingerprint and generates an analog or digital signal that is representative of the scanned fingerprint. According to at least one imaging technique, a grayscale image is produced of the scanned fingerprint. Each pixel of the grayscale image has a value between 0 and 255 -- a value of 0 value representing a "black" pixel and a value of 255 representing a white pixel. Based on this grayscale image, biometric information is extracted.

FIG. 1 shows a diagram of a known fingerprint imaging device 2. In normal operation, the fingerprint imaging device uses techniques derived from Coulombs law to determine the location of ridges and valleys in a fingerprint surface. By modeling each sensing element on the sensor as one plate in a capacitor and the finger surface (that is, the ridges and valleys) as the second plate in the capacitor, it is possible to measure a relative distance between the ridges and valleys to construct the fingerprint.

As is shown in FIG. 2, the fingerprint imaging device 2 is typically embodied in biometric sensor chip 4, which consists of an m by n array of sensing elements or capacitive plates 6.

A drawback to known biometric sensing devices, and in particular the imaging techniques employed, is that from individual to individual, and indeed, from situation to situation, the characteristics of the biometric, that is, the finger, can vary greatly. For instance, the moisture content of the finger may vary, as can the relative distance between ridges and valleys. Because these parameters vary, the resultant biometric

image may not have the requisite image clarity needed when the biometric sensing device is deployed in a highly sensitive environment.

SUMMARY OF THE INVENTION

An automatic gain amplifier is disclosed that dynamically improves the quality of scanned biometric information. According to one embodiment, an image distribution of the scanned biometric is generated. Next, areas of higher image distribution are identified. An iterative process of adjusting the gain of a biometric sensor device, for instance, a capacitive sensing element, is employed until an optimum separation of the areas of higher image distribution is achieved. Once the optimum separation is achieved, the biometric sensing device analyzes the resulting image so that biometric information can be detected with improved image clarity and less interference with noise, such as dust and changing biometric parameters. Electronic circuitry and software for implementing the methods and apparatuses of the invention are disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 depicts the operational theory behind a known biometric sensing device.

FIG. 2 depicts a known fingerprint sensor.

FIG. 3 is a histogram showing the distribution of certain pixel-values sensed by a biometric sensing device.

FIG. 4 shows a conceptual diagram of the distribution of certain pixel values as inverted according to an embodiment of the invention.

FIG. 5 shows a conceptual diagram of the distribution of certain pixel values after having adjusted a gain of the biometric sensing device according to an embodiment of the invention.

FIG. 6 shows the desired distribution of certain pixel-values after having adjusted the gain of the biometric sensing device according to an embodiment of the invention.

FIG. 7 is an electrical schematic of the automatic gain amplifier according to an embodiment of the invention.

FIG. 8 is a block diagram of a microprocessor that can programmatically modify the gain of the automatic gain amplifier according to an embodiment of the invention.

FIG. 9 is a flowchart depicting the steps performed according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. 3 is a histogram 10 showing the pixel values collected by a biometric sensor device. The figure will be used to explain how the automatic gain amplifier of the present invention operates. The histogram 10 plots the frequency (or "counts") of certain grayscale pixel values (or "pixel data") as sensed by a biometric sensor device. The x-axis has an 8-bit range of grayscale values: 0 representing black, 255 representing white, and shades of gray in between. The y-axis corresponds to the frequency of occurrence of the corresponding x-axis values.

The distribution curve 12 can be said to show three regions. The first region 14 represents noise, as does the third region 18. However, the second or "target" region 16 represents fingerprint minutiae information, such as the ridges and valleys of a fingerprint. Because fingerprints are often dry, there is a tendency for the ridges and valleys of the fingerprint to cluster near the white side of the histogram 10 when it is scanned by the biometric sensor device. The clustering tendency is illustrated by line 24, which slices through the peak 20 of the true fingerprint pixel data, and the line 26, which slices through the peak 22 of the white noise pixel data. Peaks 20 and 22 are initially separated by a distance (d) 25. The invention seeks to counteract this clustering tendency and thereby improve the clarity and resolution of the sensed biometric image.

To this end, an automatic gain amplifier is disclosed that separates the first peak 20 and the second peak 22 by iteratively adjusting the gain of an amplifier that adjusts the sensitivity of the biometric sensor device. FIGS. 4-6 are diagrammatic representations of the gain adjustment process that is described in further detail with reference to FIG. 8 (below).

Turning to FIG. 4, the histogram 10 is first inverted to histogram 30. Inverting the histogram 10 places the second peak 22 before the first peak 20 and the noise region 14 at the trailing end of the histogram 30.

Next, as is shown FIG. 5, the gain of the operational amplifier is adjusted to yield histogram 32. Adjusting the gain of the operational amplifier causes peaks 22 and 20 to separate by a distance 25'. Because the histogram 10 was inverted, the pixel values for the target region 16 are greater than the pixel values for the noise region 18. Thus, amplifying the pixel values will have the affect of spreading the lower value regions less than the upper value regions. Thus, the resolution of the target region 16 is increased more than the corresponding resolution of the noise region 18. Moreover, the noise region 14 will amplify out of range of the grayscale value -- effectively filtering it from consideration.

Now, FIGS. 4 and 5 were conceptual diagrams. Histograms 30 and 32 were actually not generated by the electronics circuitry per se, but rather through software manipulation of the fingerprint pixel data sensed by the biometric sensor device. The histograms 30 and 32 are used for the purpose of explaining the automatic adjustment process, which, according to one embodiment, is performed by a microprocessor and corresponding control software. FIG. 6, however, shows the modified histogram 34 (histogram 32 inverted) resultant from the automatic gain amplification processes described above (and in further detail below). Notice the separation of the peaks 20 and 22. Moreover, notice that the distribution area of the target region 16 is elongated -- meaning that a higher resolution and improved biometric minutiae information clarity is achieved.

FIG. 7 shows electronic circuitry that comprise a significant portion of an embodiment of the automatic gain amplifier 36 according to one embodiment of the invention. Bias voltage (V_{bias}) 40, sample voltage (V_a) 42, and sample voltage (V_b) 44 are fed into the operational amplifier 38. The voltage inputs are not always coupled to the operational amplifier 38. Instead a series of intervening switches 52 and 54, under control of opposite edges of a clock cycle (not shown), dictate whether the voltage inputs are coupled and also determine whether any intervening capacitors are charging or discharging. According to one embodiment, the sample voltages 42 and

44 represent the charge at a sensing element in a capacitive sensor chip at two separate time intervals.

A first capacitor (C_1) 46 is connected in series with bias voltage 40 and the negative input 39 of the operational amplifier 38. A second capacitor (C_2) is connected between the sample voltage 42 and sample voltage 44, and through switches 54 to the positive input 41 and negative input 39. A third, variable capacitor (C_3) 50, under control of a microprocessor executing software code or hard-wired logic circuitry, is connected between the negative input 39 and the output 56 of the operational amplifier 38. A second feedback line 51, under control of switch 52, is also connected between the negative input 39 and the output 56.

The voltage output 56 of the automatic gain amplifier 36 is represented by EQ. 1.

$$V_{out} = \frac{C_1 \cdot V_{bias} + C_2(V_b - V_a)}{C_3} \quad (1)$$

Selecting a value C for the first capacitor 46 and second capacitor 48 yields a gain for the automatic gain amplifier 36 that is inversely proportional to the variable capacitor 50 (that is, $G_m = C/C_3$).

According to one embodiment, an 8-bit analog-to-digital converter is coupled to the voltage output 56. The 8-bit analog-to-digital converter converts the analog voltage output 56 into a value that can be used by a microprocessor as an input to a software control algorithm. Alternatively, the conversion can take place at the microprocessor.

FIG. 8 depicts a microcontroller 58 that controls the variable capacitor 50. The microcontroller includes a microprocessor 60, a persistent memory 62, and a volatile memory 64, each connected through a common bus 61 to the microprocessor 60. The microcontroller 58 further includes an input/output interface 66. Fingerprint pixel data 56 is input through input line 68, for example from voltage output 56, into the microprocessor 60. The microprocessor 60 stores the values in volatile memory 64 (or in an internal microprocessor memory) and executes software code, stored in persistent memory 62, to manipulate and analyze the fingerprint pixel data 56. The result is an output signal 70 that is used to control the variable capacitor 50. The

output signal 70 can be an analog or digital signal, so an intervening digital-to-analog converter may be employed.

FIG. 9 is a flowchart depicting the steps performed by the microcontroller 58 as it manipulates and analyzes the pixel data input to control the variable capacitor 50. According to one embodiment, many of the steps are implemented in executable object code or another computer readable medium that is used to cause a microprocessor to perform the sequences of steps. For example, if the microcontroller 58 is utilized, the executable software code can be stored in persistent memory 62 and run from an execution memory area of the microprocessor 60.

In step 72, the biometric sensor device scans biometric information from, for example, a finger. The biometric image sensor device can be a capacitive fingerprint sensor or an optical fingerprint sensor. A presently preferred biometric image sensing device that can generate the pixel-values is the capacitive fingerprint sensing device disclosed in U.S. Patent Nos. 6,016,355 and 6,049,620. The capacitive fingerprint sensing device can also include a finger sensing element that enables the biometric sensor device, such as the device described in co-pending U.S. Patent Application Serial No. 09/561,174 entitled "METHOD AND APPARATUS FOR DETECTING THE PRESENCE OF A FINGER ON A BIOMETRIC SENSING DEVICE", filed on April 27, 2000.

In step 74, the biometric information is transformed into pixel-based image data, for example a grayscale value. In step 76, the frequency of the pixel values are counted, thus creating the histogram described above with references to FIG. 3. In step 78, two pixel values are selected as occurrence peaks, meaning they represent the peaks 20 and 22 described above. The selection of the occurrence peaks 20 and 22 effectively divides the histogram into the three regions. In step 80, the separation between the peaks is determined, and in step 82 the separation value is compared against a threshold separation value (or values).

According to experiments by the inventors, acceptable separation values, when using 8-bit pixel values, are between 30 and 128 pixel values. In practice, a separation value of approximately 128 is ideal when 8-bit grayscale values store the pixel data.

If the separation value is below the threshold separation value, then the capacitance of the variable capacitor 50 is adjusted in step 84. For instance, if the target region 16 and the noise region 18 are still too close, then the gain is increased, but if they are too far, then the gain is decreased.

According to one embodiment, an iterative successive approximations technique is used in step 84 whereby the capacitance adjustments are either halved or doubled depending on how the pixel data responds to the amplification. Assume, for example, that variable capacitance 50 corresponds to an 8-bit value. If the separation distance is too close, then the gain is increased by 128 units. If, upon the next pass through steps 72-82, the separation distance is too far, then the gain is decreased by 64 units. And, after the next pass through steps 72-82, if the separation distance is too close, then the gain is increased by 32 units, and so on until the ideal separation is achieved. According to other embodiments, a linear, a non-linear, a lookup-table based, or a fuzzy logic type control methodology can be implemented to adjust the output controlling the variable capacitance 50.

After step 82, if the separation value was within the threshold value (or values), then in step 86 the pixel values can then be further analyzed for specific biometric information, for instance fingerprint ridge end points or bifurcations. The specific biometric information can be used to enroll the particular biometric into a verification system, or it can be matched against enrolled biometric information stored in templates. Techniques for analyzing or matching the biometric information are disclosed in co-pending U.S. Patent Application Serial Nos. 09/354,929, filed July 15, 1999, and 09/501,355, filed February 9, 2000.

Minor modifications to the invention are envisioned, but are not necessary for the proper operation of the automatic gain amplifier described herein. For instance, anti-spoofing technology may be employed either before or after adjusting the gain, such as the anti-spoofing technology described in U.S. Provisional Application Serial No. 60/158,458, filed October 7, 1999. Moreover, the histogram 10 may be filtered at either end of the pixel values before minutiae are extracted. Similarly, the collection of pixel values for selecting a sample set for the histogram 10, or indeed even adjusting the gain itself, may be performed on a row by row, column by column, or even sub-region basis on the biometric sensor device. Accordingly, the written

description and drawings are to be interpreted in an illustrative rather than a restrictive sense and are to be limited only by the accompanying claims.

CLAIMS

What is claimed is:

1. A method for implementing an automatic gain amplifier in a biometric sensing device, comprising:

sensing biometric information from said biometric sensing device;

transforming said sensed biometric information into a pixel-based image corresponding to said biometric information;

counting a frequency of occurrence of pixel-values in said pixel-based image;

selecting at least two of said counted frequency of occurrence of pixel-values as a first peak and a second peak;

determining a separation pixel-value between said first peak and said second peak; and

adjusting a gain amplifier coupled to said biometric sensing device in an iterative manner until said second peak is not less than thirty separation pixel values from said first peak.

2. The method of claim 1, wherein said biometric sensing device comprises a capacitive fingerprint sensor.

3. The method of claim 2, wherein said capacitive fingerprint sensor comprises a finger sensing element configured to enable said biometric sensing device when a finger is present.

4. The method of claim 1, wherein said biometric sensing device utilizes an optical fingerprint sensor.

5. The method of claim 1, wherein adjustment of the automatic gain amplifier is performed by a microcontroller.

6. The method of claim 5, wherein the microcontroller has input comprising said pixel-values and an output comprising a signal that controls gain of said gain amplifier.

7. The method of claim 6, wherein said input to said microcontroller corresponds to a charge differential at a capacitive sensing element over a fixed period, and in response to said charge differential, performs said step of adjusting said gain of said gain amplifier.

8. The method of claim 7, wherein said charge differential is measured in a two phase process.

9. The method of claim 1, wherein said step of iteratively adjusting said gain amplifier is accomplished by adjusting a capacitance value of a variable capacitor within said gain amplifier.

10. The method of claim 9, wherein said step of adjusting said capacitance value of said variable capacitor is accomplished in a successive approximations manner.

11. The method of claim 9, wherein one or more steps of iteratively adjusting said gain amplifier are stored in object code in a persistent memory.

12. The method of claim 1, further comprising analyzing said pixel-values for specific biometric pattern information when said separation pixel-value is within a specified threshold.

13. A computer software product configured to cause one or more processors to perform the steps in any of above claims 1-12.

14. An automatic gain amplifier for a biometric sensing device, said automatic gain amplifier comprising:

an operational amplifier having a negative input, a positive input and an output;

a bias voltage input coupled to said negative input through a first capacitor;

a first biometric voltage input coupled to said negative input;

a second biometric voltage input coupled to said positive input, said first biometric input voltage and said second biometric input voltage coupled through a second capacitor;

a programmable capacitance coupled between said negative input and said output, said programmable capacitance inversely proportional to a gain of said automatic gain amplifier; and

a microcontroller communicatively coupled to said programmable capacitance, said microcontroller configured to iteratively adjust said programmable capacitance, said iterative adjustments dependent upon a separation pixel-value between a first peak and a second peak in a pixel-value frequency distribution generated from a plurality of biometric sensing elements in said biometric sensing device.

15. The automatic gain amplifier of claim 14, wherein said microcontroller comprises:

a microprocessor;

a persistent memory;

a volatile memory, each connected through a common bus to the microprocessor; and

an input/output interface communicatively connected to said microcontroller, said input/output interface having an input and an output, said input configured to receive pixel data, said output configured to drive a signal used to adjust a capacitance of said programmable capacitance.

16. The automatic gain amplifier of claim 15, wherein said pixel data received through said input is stored in said volatile memory.

17. The automatic gain amplifier of claim 14 wherein said biometric sensing device comprises:

a sensor chip having an array of capacitive sensing elements;

a biometric contact surface disposed above said array of capacitive sensing elements; and

a passivation layer disposed between said sensing elements and said biometric contact surface.

18. The automatic gain amplifier of claim 14, wherein adjusting said programmable capacitance increases clarity of a pixel-based image created from said plurality of biometric sensing elements.

19. A method for controlling image clarity in a biometric sensing device, comprising:

receiving biometric information from said biometric sensing device;

transforming said sensed biometric information into a pixel-based image comprised of pixel-values corresponding to said biometric information;

counting a frequency of occurrence of said pixel-values in said pixel-based image;

selecting at least two of said counted frequency of occurrence of said pixel-values as a first peak and a second peak;

determining a separation pixel-value between said first peak and said second peak;

inverting said pixel-values;

calculating an adjustment value based on said separation pixel-value; and

adjusting a gain of said biometric sensing device corresponding to said adjustment value.

20. The method of claim 18, further comprising repeating claim 18 until said separation-pixel value is within a specified threshold.

21. The method of claim 19, further comprising analyzing said plurality of pixel-values for specific biometric pattern information when said separation pixel-value is within said specified threshold.

22.. The method of claim 18, wherein said steps of reading biometric information from said biometric sensing device and transforming said sensed biometric information into a pixel-based image comprised of pixel-values comprises:

sampling a first charge at a capacitive plate;

discharging said capacitive plate for a fixed period of time;

sampling a second charge at said capacitive plate after said fixed period of time;

measuring a difference in charge between said first charge and said second charge; and

transforming said difference in charge into one of said pixel-values.

23. A computer software product configured to cause one or more processors to perform the steps in any of above claims 1-12 or 19-22.

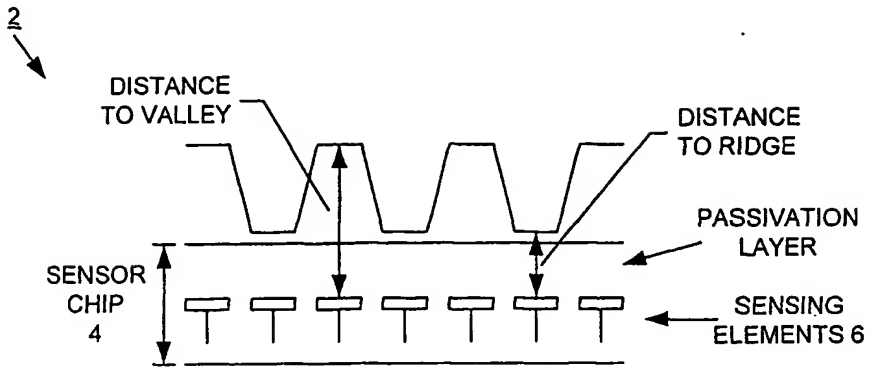

2
DISTANCE TO VALLEY
DISTANCE TO RIDGE
PASSIVATION LAYER
SENSOR CHIP 4
SENSING ELEMENTS 6

FIG. 1

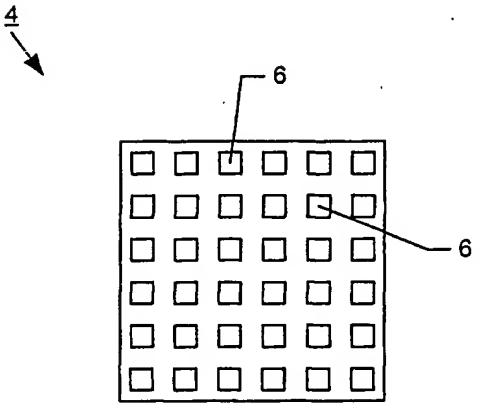

4
6
6

FIG. 2

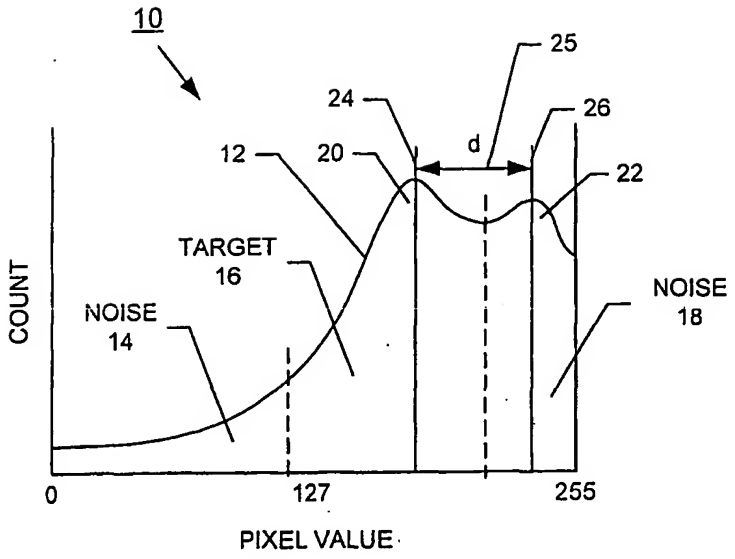

10
25
24
26
d
12
20
22
TARGET
16
NOISE
14
NOISE
18
COUNT
0
127
255
PIXEL VALUE

FIG. 3

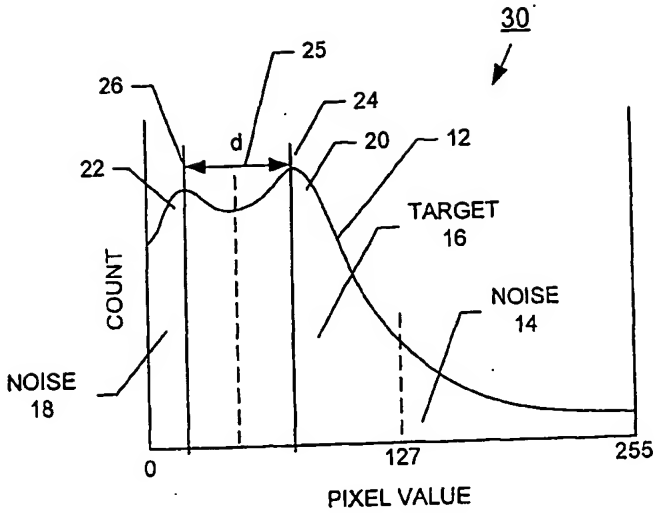


FIG. 4

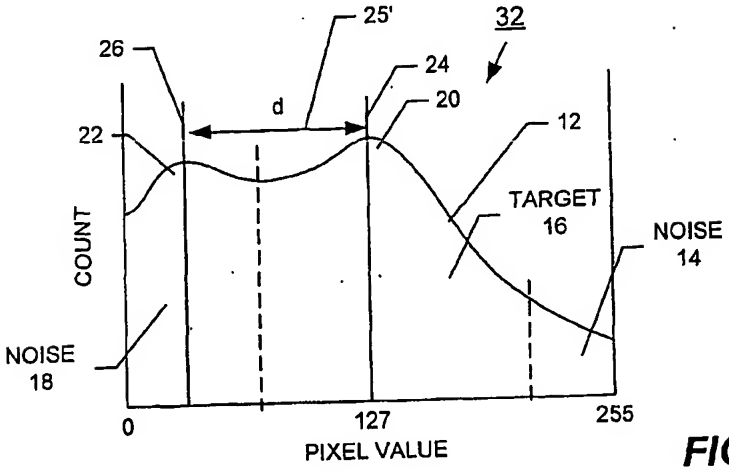


FIG. 5

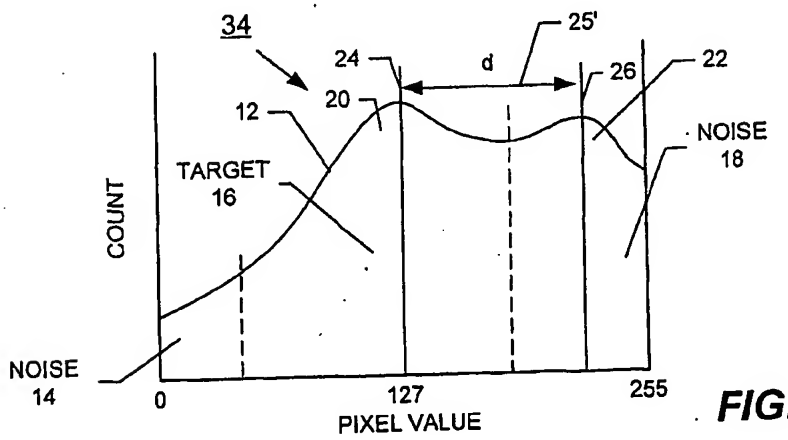


FIG. 6

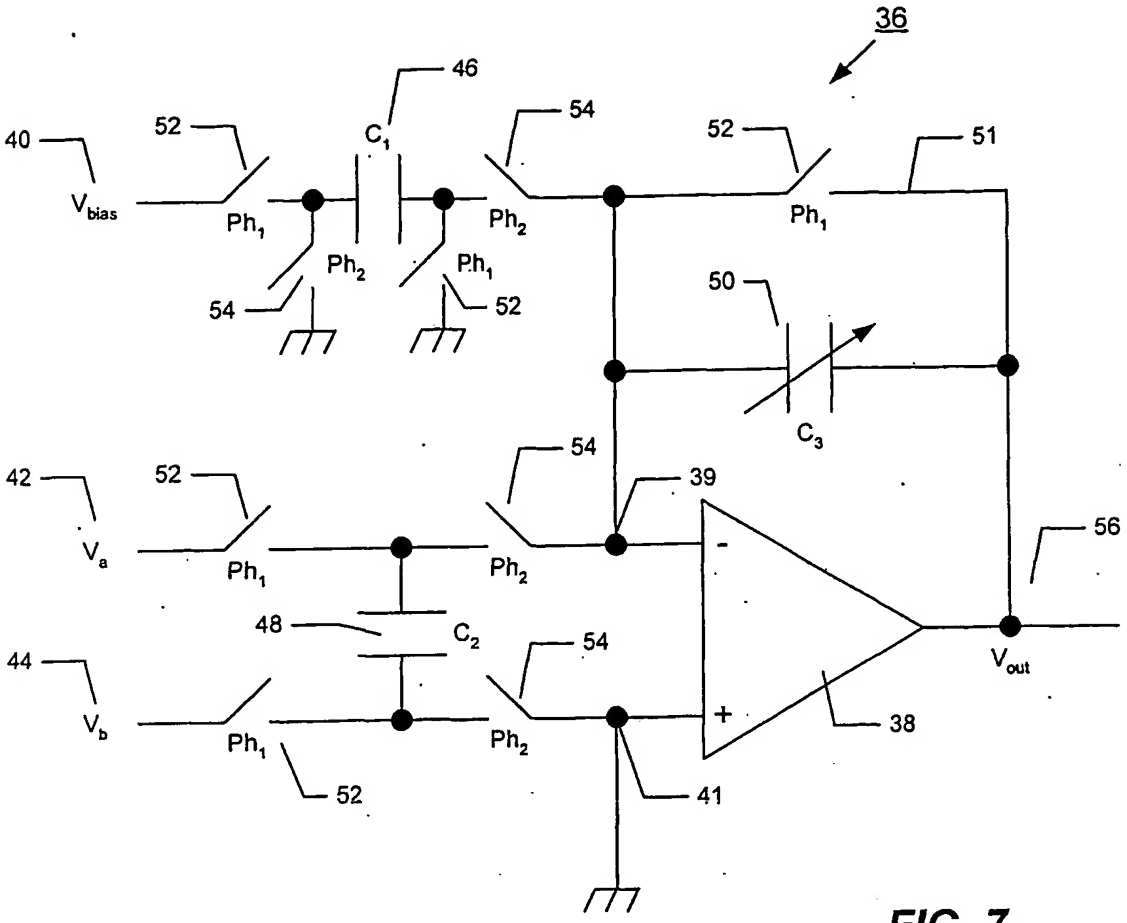

36
46
40
52
C_1
54
52
51
V_{bias}
Ph_1
Ph_2
Ph_1
Ph_2
Ph_1
54
52
50
C_3
42
52
54
39
56
V_a
Ph_1
Ph_2
48
C_2
54
44
V_{out}
V_b
Ph_1
Ph_2
38
52
41

FIG. 7

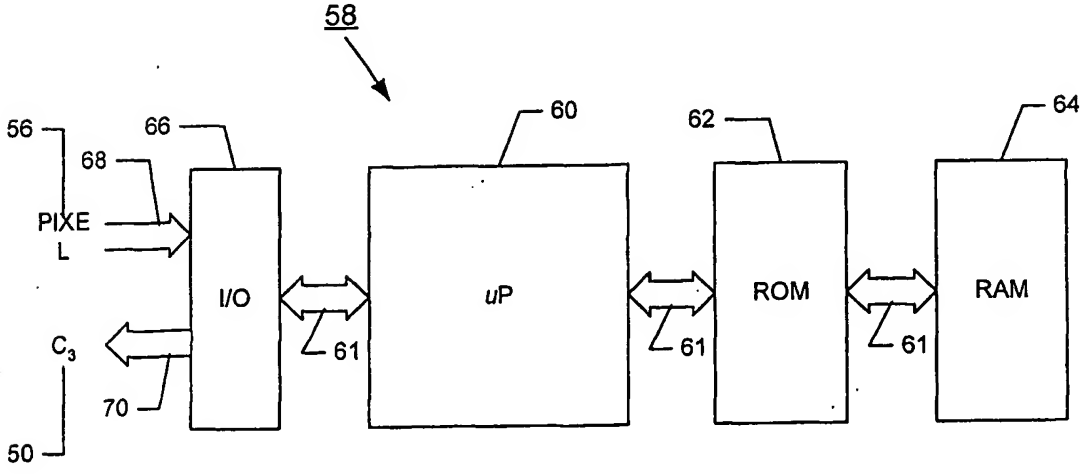

58
56
66
60
62
64
68
PIXEL
I/O
uP
ROM
RAM
C_3
61
61
61
70
50

FIG. 8

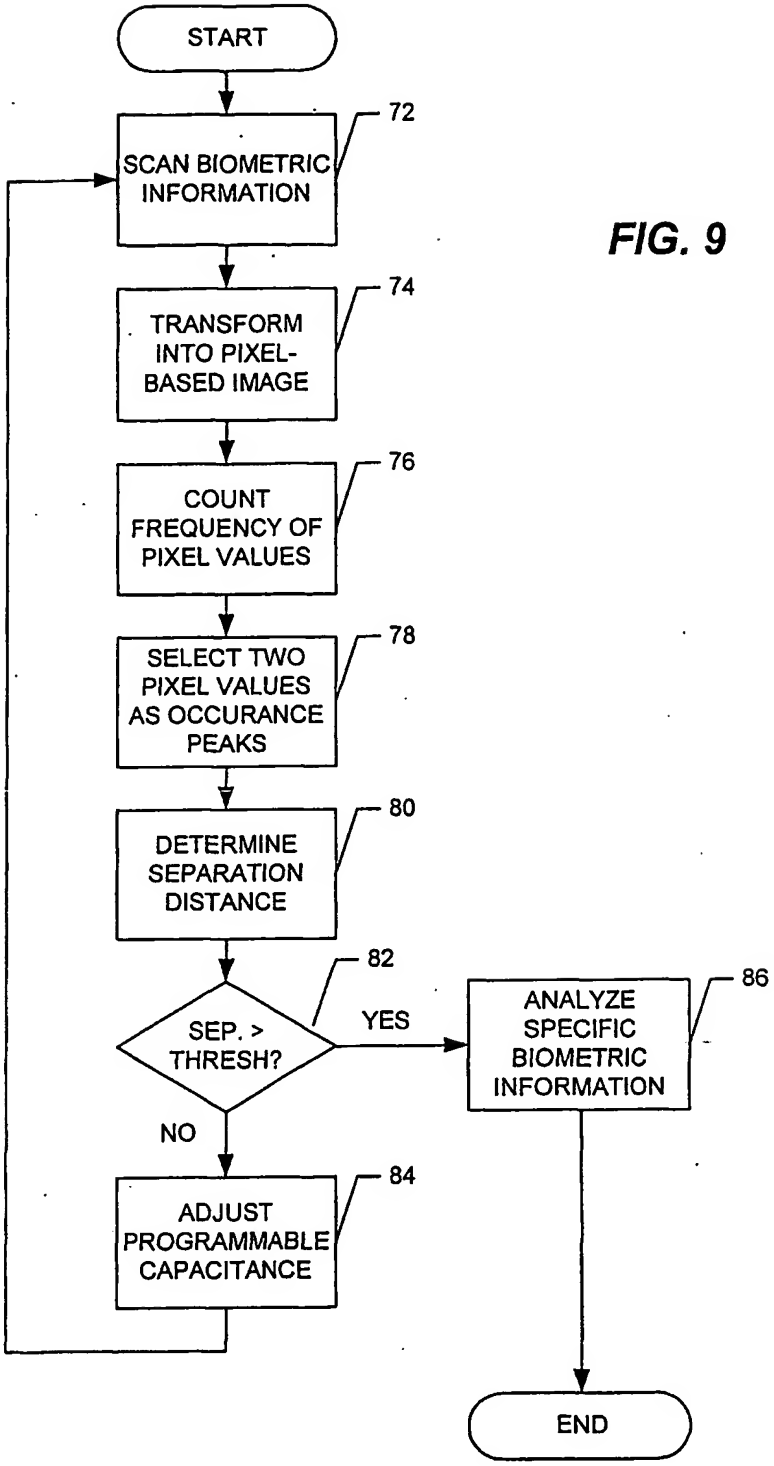

START
SCAN BIOMETRIC INFORMATION
72
TRANSFORM INTO PIXEL-BASED IMAGE
74
COUNT FREQUENCY OF PIXEL VALUES
76
SELECT TWO PIXEL VALUES AS OCCURANCE PEAKS
78
DETERMINE SEPARATION DISTANCE
80
SEP. > THRESH?
82
YES
NO
ANALYZE SPECIFIC BIOMETRIC INFORMATION
86
ADJUST PROGRAMMABLE CAPACITANCE
84
END

FIG. 9